Modeling Payments Regulation and Financial Change

*Matthew W. Swinehart**

INTRODUCTION

The dominant narrative about changes in financial technology—or "fintech" in today's gushing parlance—is that the financial services industry is undergoing nothing short of a revolution.[1] No part of the financial sector has a better claim to that revolution narrative than payment services, which every year move more than a quadrillion—or one thousand trillion—U.S. dollars globally[2] and more than 175 trillion U.S. dollars in the United States alone.[3]

In the last two decades, payments have moved away from cash, paper checks, and other relatively slow and expensive mechanisms to incrementally faster and cheaper digital payment services. Digital payments now account for more than 80 percent of all U.S. consumer

---

* Matthew Swinehart is the Counsel for International Trade and Financial Regulatory Policy, and Lead Financial Services Negotiator, at the U.S. Department of the Treasury. The views expressed here are the author's own and not necessarily the views of the Department of the Treasury or the United States government. The author thanks Steven Schwarcz, Ronald Mann, Christopher Bradley, Michael Radolinski, Jeff Siegel, and the participants of the 2018 National Business Law Scholars Conference at the University of Georgia School of Law.

1. *See, e.g.,* Nathaniel Popper, *Where Finance and Technology Come Together*, N.Y. TIMES (Nov. 14, 2016), https://www.nytimes.com/2016/11/15/business/dealbook/where-finance-and-technology-come-together.html [https://perma.cc/ZR6M-8LU5] (cataloguing fintech companies' assessments of their own potential). Most definitions of "fintech" in use today focus on the commercialization of new technology to a degree noticeable in the market. *See, e.g.*, FIN. STABILITY BD., FINANCIAL STABILITY IMPLICATIONS FROM FINTECH 7 (2017), http://www.fsb.org/wp-content/uploads/R270617.pdf [https://perma.cc/5BJP-7WWN] (defining "fintech" as a "technology-enabled innovation in financial services that could result in new business models, applications, processes[,] or products with an associated material effect on the provision of financial services").

2. See GOV'T ACCOUNTABILITY OFFICE, GAO-16-614, PAYMENT SERVICES: FEDERAL RESERVE'S COMPETITION WITH OTHER PROVIDERS BENEFITS CUSTOMERS, BUT ADDITIONAL REVIEWS COULD INCREASE ASSURANCE OF COST ACCURACY 1 (2016), https://www.gao.gov/assets/680/679388.pdf [https://perma.cc/S2LZ-THPD] (noting the value for the year 2015).

3. *See* FASTER PAYMENTS TASK FORCE, THE U.S. PATH TO FASTER PAYMENTS: FINAL REPORT PART ONE: THE FASTER PAYMENTS TASK FORCE APPROACH 16 (2017), https://www.federalreserve.gov/newsevents/press/other/US-path-to-faster-payments-pt1-201701.pdf [https://perma.cc/MPA7-DUFU].

purchases of goods and services and nearly 100 percent of all other commercial transactions.[4] They are essential to the efficient functioning of markets and the real economy[5] and continued U.S. economic competitiveness.[6] Given this importance, state and federal regulators have created a well-established framework over the last several decades to protect consumers from unfair practices and unauthorized transactions, to prevent criminals and terrorists from using payment services, and to preserve the safety and soundness of the larger financial system.[7]

A common corollary to the revolution narrative is that financial change—both change in the technologies and change in the business models of financial services companies—will require a broad rethinking of financial regulation. According to this corollary, a failure of financial regulators to adapt to these developments will reduce the competitiveness of domestic financial services firms, hinder efforts to increase basic access to financial services, and even undermine their own regulatory objectives.[8]

This Article challenges that logic as it applies to payment services. The motivating insight here is that payments regulation is largely technology-neutral and activity-based and thus readily capable of

---

4. *See* FED. RESERVE BD., FEDERAL RESERVE PAYMENTS STUDY 3 (2016), https://www.federalreserve.gov/newsevents/press/other/2016-payments-study-20161222.pdf [https://perma.cc/TDQ5-TUMZ] (noting nearly $150 trillion in digital payments and $26.83 trillion in paper checks in 2015). The use of paper checks (by number) peaked in the mid-1990s. *See id.* at 4.

5. *See* Marc Rysman & Scott Schuh, *New Innovations in Payments*, 17 INNOVATION POL'Y & ECON. 27, 27 (2017).

6. *See* FASTER PAYMENTS TASK FORCE, FINAL REPORT PART TWO: A CALL TO ACTION 3 (2017), https://fedpaymentsimprovement.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf [https://perma.cc/G63Y-7RNE] ("The payment system is critical to the economic vitality and competitiveness of the United States and must continually evolve to meet the needs of an economy that is becoming more global, digitally-interconnected, real-time and information-driven."); *see also* COMM. ON PAYMENT & SETTLEMENT SYS., BANK FOR INT'L SETTLEMENTS, INNOVATIONS IN RETAIL PAYMENTS 24 (2012) [hereinafter BIS/CPSS, INNOVATIONS IN RETAIL PAYMENTS], https://www.bis.org/cpmi/publ/d102.pdf [https://perma.cc/J6AZ-UBSX] (reporting the results of studies showing potential gains in a country's annual GDP between one-quarter of one percent and one percent).

7. *See infra* Part III.

8. *See, e.g.*, CHRIS BRUMMER & DANIEL GORFINE, CTR. FOR FIN. MKTS., MILKEN INST., FINTECH: BUILDING A 21ST-CENTURY REGULATOR'S TOOLKIT 1 (2014), https://assets1b.milkeninstitute.org/assets/Publication/Viewpoint/PDF/3.14-FinTech-Reg-Toolkit-NEW.pdf [https://perma.cc/UBX3-JV2N] (arguing that "the rise of FinTech challenges underlying precepts of existing regulatory approaches and requires fresh thinking as to how regulation can best foster the responsible development of this industry" and "outlin[ing] characteristics of FinTech that drive the need for new thinking about today's regulatory approaches"); *id.* ("A failure to account for these trends will result in regulatory frameworks that fall short of their goals, impede positive innovation, and reduce competitiveness of local economies and businesses."); *id.* at 14 ("The novel features of FinTech innovation will . . . . . require a re-thinking of how we approach regulation and the processes we apply to rulemaking.").

adapting to financial change. The Article constructs a stylized model—the "payment stack"—to place incumbents, sources of financial change, and regulatory objectives together in context. The model sorts all payment services into seven categories based on their function within the larger payments ecosystem. Relying on this model, the Article concludes that services within each category are subject to roughly equivalent regulation (or subject to no payments regulation), irrespective of the underlying technology or choice of business strategy.[9] Because that regulation maps onto the underlying economic functions of payment services, it is largely technology-neutral and activity-based, making it less time-dependent and more durable in the face of industry innovation.[10]

This Article constructs and operationalizes the payment stack model in five parts. Part I briefly outlines the functions of payment services and the core objectives of current U.S. payments regulation.[11] Given the considerable heterogeneity in payments markets and regulation across the globe, this Article does not seek to apply the model outside of the United States.

Part II sorts the activities that make up the payments ecosystem into layers according to their functions and interdependencies in a payment transaction. In sorting services according to their functions and interdependencies, the payment stack model borrows from two distinct sources. The first source is the concept of a "stack": a modeling method

---

9. Others have made related arguments about the activity-based nature of certain aspects of financial regulation as applied to certain technologies. *See, e.g.*, Mills et al., *Distributed Ledger Technology in Payments, Clearing, and Settlement* 27–28 (Fed. Reserve Bd. Fin. and Econ. Discussion Series, Working Paper No. 2016-095, 2016), https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf [https://perma.cc/J2NL-KFLH] ("The relevant laws, regulations, and supervisory policies [with respect to distributed ledger technology] are aimed at achieving broad objectives such as market transparency, safety and soundness of financial institutions, and the efficient and effective functioning of the broader financial system, and are not generally intended to favor a particular electronic technology."); Larry D. Wall, *Avoiding Regulation: FinTech Versus the Sharing Economy*, FED. RES. BANK ATLANTA (Sept. 2016), https://www.frbatlanta.org/cenfis/publications/notesfromthevault/09-avoiding-regulation-fintech-versus-the-sharing-economy-2016-09-29.aspx [https://perma.cc/BN8R-CMXJ] ("[M]any of these [financial regulation] rules are written so they cover not only banks and other traditional financial firms but would also cover fintech firms."). This is a point that many fintech firms often use to counter assertions that they are unregulated under current regimes. *See, e.g.*, Jerry Brito, *Is Bitcoin Regulated?*, COIN CTR. (Jan. 13, 2015), https://coincenter.org/entry/is-bitcoin-regulated [https://perma.cc/6HYS-8V57].

10. *See* Steven L. Schwarcz, *Regulating Financial Change: A Functional Approach*, 100 MINN. L. REV. 1441, 1444 (2016).

11. *See generally* COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, BANK FOR INT'L SETTLEMENTS, NON-BANKS IN RETAIL PAYMENTS (2014) [hereinafter BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS], https://www.bis.org/cpmi/publ/d118.pdf [https://perma.cc/TMJ9-M3ZL].

to create visual relationships among dependent elements of a system. The original stack model—the "internet protocol stack"—showed how various internet protocols built on one another so that hardware and software can communicate in ways that are intuitive to humans.[12] The second source for the payment stack model is the longstanding observation in legal scholarship that a focus on the functions of regulated activities—who provides a service, to whom, and how, for example—is essential to understanding the relationship between regulation and a rapidly changing system.[13]

Relying on this functional stack model, Part III describes the existing scope of regulation that applies to activities in each layer of the stack and assesses the degree to which that regulation is technology-neutral and activity-based. Regulation that follows such an approach, by seeking to regulate similar risks in a similar manner, not only allows regulators to adapt more quickly to new challenges, even in times of immense change, but also enhances predictability, assures market participants and their customers that regulators are focused on risk rather than extraneous considerations, reduces incentives to engage in regulatory arbitrage, and provides a level regulatory playing field.[14]

The model constructed here demonstrates that payments activities

---

12. Henrik Frystyk, *The Internet Protocol Stack*, WORLD WIDE WEB CONSORTIUM (July 1994), https://www.w3.org/People/Frystyk/thesis/TcpIp.html [https://perma.cc/Y8XS-DXXQ].

13. *See* Schwarcz, *supra* note 10, at 1444; Robert C. Merton & Zvi Bodie, *A Conceptual Framework for Analyzing the Financial Environment*, *in* THE GLOBAL FINANCIAL SYSTEM: A FUNCTIONAL PERSPECTIVE 6, 10–11 (Dwight B. Crane et al. eds., 1995).

14. *See* U.S. DEP'T OF TREASURY, FINANCIAL STABILITY OVERSIGHT COUNCIL DESIGNATIONS 9 (2017), https://www.treasury.gov/press-center/press-releases/Documents/PM-FSOC-Designations-Memo-11-17.pdf https://perma.cc/HBZ2-TVUD] ("Firms engaged in the same activity should be treated uniformly based on how the activity may contribute to risk. Failure to do so could distort free markets."); FIN. STABILITY BD., *supra* note 1, at 2–3 ("Regulators should be agile when there is a need to respond to fast changes in the FinTech space. This may be more easily and efficiently achieved with an approach that is neutral with regard to technologies and based on financial service activities."); C. Andrew Gerlach et al., *U.S. Regulation of FinTech – Recent Developments and Challenges*, 44 CAPCO INST. J. FIN. TRANSFORMATION 87, 90 (2016) ("By seeking to ensure that comparable financial products and services are regulated similarly, regardless of the nature of the provider, regulators seek to minimize the opportunity for regulatory arbitrage."); BIS/CPSS, INNOVATIONS IN RETAIL PAYMENTS, *supra* note 6, at 55 ("At the same time, a balanced regulatory approach is necessary to prevent inconsistencies between regulatory requirements already established for different providers and industrial sectors. Furthermore, a level playing field for banks and non-bank providers is essential to avoid competitive distortions."); *see also* Comments of Funding Circle on the Office of the Comptroller of the Currency's Proposal for Special Purpose National Bank Charters for Fintech Companies 3 (Jan. 17, 2017), https://www.occ.treas.gov/topics/responsible-innovation/comments/comment-funding-circle.pdf [https://perma.cc/LG2A-NEB8] ("Regulatory parity among companies, new and incumbent, that engage in the same business activities is not only a matter of fairness, but also drives more market participants to operate under the same rulebook.").

within each stack layer are subject to roughly equivalent regulation, irrespective of the type of technology or business model involved. And many payment activities subject to a significant degree of financial change do not pose payment-specific risks and are thus subject to only limited regulation in the first place. This suggests that financial change will not demand wholesale changes to payments regulation, defying today's prevailing narrative about financial services in general.

But that is not to say that payments regulation should be static. Because the basic structure of existing approaches is relatively durable, as outlined in Part IV, payments regulators have the opportunity to follow a nuanced, fact-specific approach rather than a broad agenda of reform. In response to some forms of financial change, regulators may need simply to make explicit that existing regulation applies to that change. Other forms of financial change might provide regulators with an opportunity to correct the limited aspects of payments regulation that are not entirely neutral with respect to technology or business model. And with yet other forms of financial change, regulators may need to take further steps, including in circumstances in which regulation becomes obsolete in the future due to forms of "payment stack collapse," the fragmented nature of the payments market impedes market-based improvements, change results in an activity that is inherently low-risk, or change actually improves the ability of regulators to achieve their objectives.

I. ESSENTIALS OF PAYMENT SERVICES AND THEIR REGULATION

Before constructing the payment stack model, it is useful to outline the basic utility of payment services—what they do and why—and the core objectives of payments regulation.

A. The Utility of Payment Services

In theory, the U.S. economy could function without digital payment services. There is no absolute need for them, and there are other ways of moving wealth around the economy. Consumers and businesses could, for example, use physical cash to pay for everything.[15] Cash is convenient in many ways: when a consumer pays with cash, the merchant receives final payment in a form that it can immediately use to

15. Although not typically considered a payment service in legal scholarship, the production, distribution, and redemption of physical payment instruments, including cash, is in some limited senses a government-supplied payment service.

make payments of its own, without further processing, transformation, or recording of the transaction.[16] But cash is difficult to carry around in large amounts and to use securely, and consumers, businesses, and regulators may prefer that a transaction generate a record that proves the payment was made.[17] Digital payments reduce these frictions inherent to economic transactions and, by moving money more efficiently than physical cash, improve the functioning of the real economy.

Three characteristics define the current digital payments market in the United States in ways that may affect the nature and degree of financial change in the market. The first characteristic is that the U.S. payments market is relatively saturated, with an established set of incumbent services and providers. Incumbency in the payments market matters to a large degree because every payment service must, either alone or together with other payment services, operate as a multisided platform that is capable of matching payment senders with payment recipients.[18] Through this matchmaking function, a payment service connects consumers with merchants (person-to-business or business-to-person payments, usually in connection with the exchange of goods or services), individuals with other individuals (peer-to-peer payments), or businesses with other businesses (business-to-business payments).

Today's incumbents enjoy a large network of participants—consumers, merchants, and banks, for example—that provides a number of key advantages. These include supply-side advantages due to economies of scale (so that the average cost of providing payment services falls as they provide more services) and demand-side advantages due to an existing critical mass of end-users (so that the addition of each new end-user increases the utility of the network for all users and provides incentives for more consumers and merchants to also join the network).[19] Incumbents have cemented these advantages through a complex network of contracts among participants and shared

16. RONALD J. MANN, PAYMENT SYSTEMS AND OTHER FINANCIAL TRANSACTIONS 3–4 (6th ed. 2016).

17. *Id.* at 4.

18. *See* DAVID S. EVANS & RICHARD SCHMALENSEE, MATCHMAKERS: THE NEW ECONOMICS OF MULTISIDED PLATFORMS 1–2, 149–64 (2016). A person or entity that is owed money is sometimes called a "payer," while a person or entity that is owed money is sometimes called a "payee." Either a payer or a payee may initiate payments, but those terms are not intuitive, so this Article will simplify by referring to payment senders and recipients.

19. *See* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 492–95, 512–15 (1998). Network effects in payment messaging services are well-documented. *See, e.g.*, BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 14; Ronald J. Mann, *A Requiem for Sam's Bank*, 83 CHI.-KENT L. REV. 953, 968 (2008).

technological standards.[20] New entrants thus face the significant challenge, at a very early stage, of drawing consumers, merchants, and banks away from existing players to achieve their own economies of scale and critical mass of end-users before incumbents are able to develop or acquire a competing technology or business model.[21]

The second defining characteristic of the U.S. payments market is that it is bank-centric. Banks—entities whose primary business involves commercial lending from demand deposits[22]—have historically dominated the market, which is a relatively mature one, with relatively high levels of financial inclusion and a deep bench of incumbent providers.[23] This dominance is partly a function of the relationships between banks and their commercial and investment clients, which account for the vast majority of payments volume. Although banks have also enjoyed extensive relationships with consumer clients, the market has remained susceptible to competition in consumer payments from a broad range of new technologies and business models. Changes in technology and business model have led to a proliferation of nonbank payment providers—including some of the largest companies in the world—which have improved the efficiency, security, and convenience of retail payment services, lowering transaction costs and making economic activity in all sectors more efficient.[24] At the same time, nonbanks must still rely on banks for access to the underlying payments infrastructure that the Federal Reserve and the largest banks operate.

The third key characteristic of the U.S. payments market is that it is account-based, in that payment senders and recipients must have an account that holds funds in order to access payment services. Account-based digital payments depend necessarily on the maintenance of a payment account at a bank or other account provider and that provider's ability to verify the identity of the account holder. By contrast, token-

---

20. *See* Lemley & McGowan, *supra* note 19, at 492–94.

21. *See id.* at 492–95; *see also* FIN. STABILITY BD., *supra* note 1, at 4 (noting that "network effects and economies of scale and scope could foster greater concentration" in financial services).

22. This functional definition is reflected in the definition of "bank" in U.S. statutes, which also includes any institution insured by the Federal Deposit Insurance Corporation and provides for a number of categorical exclusions. 12 U.S.C. § 1841(c) (2012). It is also the most common functional definition used in international regulatory forums. *See, e.g.*, BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 27. Bank holding companies (as well as nonbanks) may in some circumstances own entities that provide payment services and do not fit within this functional definition (e.g., specialty credit card banks). *See* Saule T. Omarova & Margaret E. Tahyar, *That Which We Call a Bank: Revisiting the History of Bank Holding Company Regulations in the United States*, 31 REV. BANKING & FIN. L. 113, 170 (2012).

23. *See* MANN, *supra* note 16, at 4.

24. *See* BIS/CPSS, INNOVATIONS IN RETAIL PAYMENTS, *supra* note 6, at 7, 15, 20.

based payments, such as bitcoin and other services that rely on distributed ledger technology, do not require any contemporaneous account verification or a network of account providers.

Each of these characteristics affects both the opportunities available to market participants when implementing financial change in payment services and the choices available to regulators in addressing that change.

B. Objectives of Payment Services Regulation

Before modeling the details of payments regulation and the possible consequences of financial change, it is critical to understand the core objectives behind government intervention in the payments market. Financial regulators have long concerned themselves with the safe and efficient functioning of payment services given their key role in the financial system and the real economy.[25] In its current form, U.S. payments regulation serves three core objectives. The first objective is the protection of individual consumers from unfair business practices or losses due to unauthorized transactions or errors. Regulators seek to achieve this "consumer protection" objective through rules governing risk allocation in individual transactions, financial requirements placed on nonbanks that provide certain consumer services, and the underlying bank regulatory regime.[26]

The second objective is to prevent criminals and terrorists from using payment services to further their illegal activities.[27] The core of this law enforcement regime in the United States is the Bank Secrecy Act,[28] originally enacted in 1970, which imposes customer due diligence, reporting, and monitoring obligations, among other requirements.[29] As with consumer protection, regulators seek to achieve this objective both through rules applicable to nonbanks and through the underlying bank regulatory regime.

The third and final objective is financial stability—ensuring the

---

25. *See* BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 1.

26. *See infra* Part III.

27. This Article will not separately address U.S. sanctions programs—which prohibit unlicensed transactions with designated entities—because they serve objectives beyond the traditional framework of financial regulation. To the extent that sanctions serve the financial regulatory objectives that are addressed in this Article, the other law enforcement regulations discussed here serve as useful proxies for understanding those objectives. *See, e.g.*, 31 C.F.R. § 560.530(a)(3) (2017) (describing certain U.S. sanctions programs).

28. Bank Secrecy Act, 12 U.S.C. §§ 1829b, 1951–59; 31 U.S.C. §§ 5311–5314, 5316–32 (2012).

29. *See infra* Section III.C.

safety and soundness of individual payment providers and payment networks, and the stability of the overall financial system.[30] Payment services companies may transmit risks because they engage as a conduit for activities that affect other participants in the financial system.[31] A financial institution that is unable to fund a payment will transmit risk to any other institution that expected payments from it over the course of the day and to any settlement service provider that extended credit to participants, and ultimately those problems may be transmitted to the real economy.[32]

The chief financial stability risks associated with payment systems are liquidity risk (the risk that a participant in the system will be unable to meet its obligations when due), credit risk (the risk that a system participant will be unable to meet its obligations at any time in the future), and operational risk (the risk that deficiencies, errors, failures, or disruptions in the hardware or software of a digital payment system will result in the reduced efficiency, security, or availability of the system's services).[33] Because banks play a central role in the payments market today, regulators primarily rely on the underlying regime of banking regulation and supervision to achieve this objective, although the U.S. government reduces liquidity and credit risks associated with settlement by operating its own systems and by applying specific rules to certain privately operated payment infrastructures.[34]

II. THE PAYMENT STACK: A FUNCTIONAL TYPOLOGY OF PAYMENT SERVICES

To better understand the potential effects of financial change on payments regulation, the payment stack model reduces the thousands of payment services and providers into seven stylized categories. The model is both activity-based, in the sense that it sorts payment services according to their function in moving wealth around the economy, and technology-and-business-model-neutral, in that the model does not take into account the particulars of the hardware or software enabling a payment service or the strategic choices and structure of the service

30. *See* FIN. STABILITY BD., *supra* note 1, at 17–21.

31. *See* Mann, *supra* note 19, at 965.

32. *See id*. at 966–67.

33. *See* FED. RESERVE BD., FEDERAL RESERVE POLICY ON PAYMENT SYSTEM RISK 4–5 (2017), https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf [https://perma.cc/B2XZ-J7N9].

34. *See infra* Sections III.D, III.F.

provider. Such a model can facilitate the analysis of systems that are subject to fast-paced changes but that depend on relatively static and familiar activities—in this case, the movement of wealth around the economy.[35] This coincides with analytical frameworks in other disciplines, including engineering and economics, which focus on the inputs and outcomes of a system, without concern for the system's internal complexity.[36]

The model also blends two distinct categories of payment services. The first category is retail payments, which are relatively low-value payments, most often between two individuals or an individual and a business.[37] The second category is wholesale payments, which are relatively high-value payments, most often between two businesses.[38] Because many retail payments are eventually settled on wholesale payment systems, it is important to understand the interplay between these two types of payments. The model, at the same time, takes into account potential differences between retail and wholesale payments that may affect regulatory responses to financial change.

As shown in Figure 1, the resulting payment stack model consists of six interdependent service categories—platform, processing, payment account, connection, messaging, and settlement services—and a seventh, standalone category, end-to-end services, which generally provide all functions necessary to complete a payment transaction. There are many other models that show the flow of digital messages from service provider to service provider. The payment stack model does not attempt to describe the specific messages that may be sent from a provider in one service category to a provider in another. The model is instead roughly organized according to the arc of most transactions, beginning at the top with the perspective of a typical individual or business end-user, and moving down through the underlying processes, invisible to most end-users, that drive the transaction.

---

35. *See* Schwarcz, *supra* note 10, at 1445; Merton & Bodie, *supra* note 13, at 6, 10–11.

36. *See* Schwarcz, *supra* note 10, at 1445 (noting that this is known as a "black-box" analysis in engineering disciplines); Merton & Bodie, *supra* note 13, at 10–11 (noting that economists refer to this analysis as a "functional perspective").

37. *See generally infra* Part II.

38. *See generally id.*

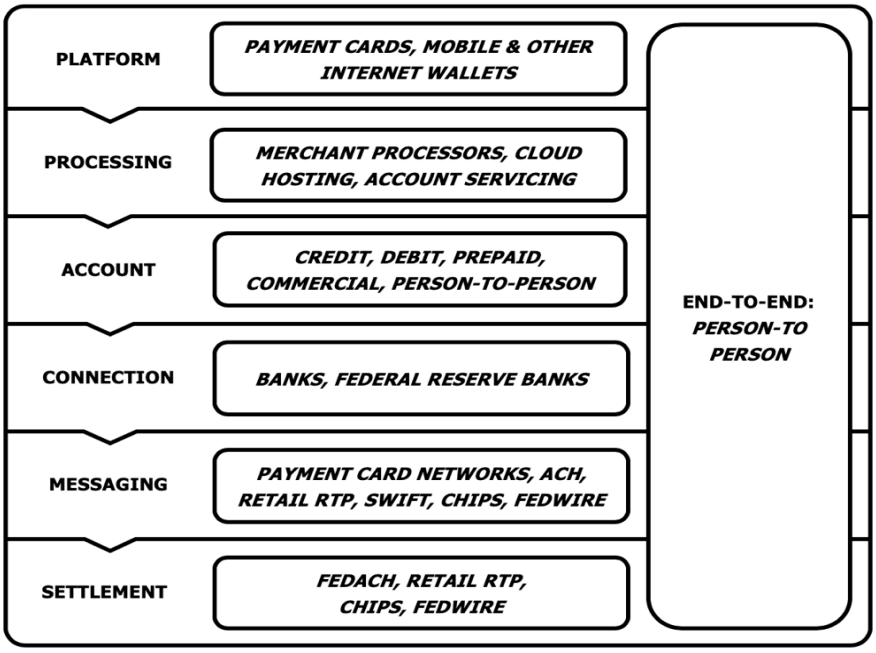

Figure 1: Payment Stack Model

Each service category serves an essential function in a payment transaction: (1) platform services allow end-users to initiate payment transactions; (2) processing services perform the complex information technology functions underlying payments; (3) account services hold funds on behalf of payment senders and recipients; (4) connection services provide relationships with banks and access to settlement infrastructure; (5) messaging services enable payment senders to communicate with payment recipients; and (6) settlement services effect the actual transfer of funds from the payment recipient to the payment sender.[39] Each of the seven categories of services in the payment stack

39. In more classical terms, digital payments typically involve five basic steps: (1) submission, (2) validation, (3) conditionality, (4) clearing, and (5) settlement. *See* Mills et al., *supra* note 9, at 5 & n.8. To send or receive funds, a payment message is submitted or sent across the payment system and then validated or authenticated, which might involve verification of the sender's identity and the integrity of the message. *See id.* at 5. If the payment message is validated, the system determines whether the payment meets the conditions for settlement, generally the availability of sufficient funds or credit. *See id.* Clearing readies the payment for settlement and involves the exchange of payment information between the service providers of the payment sender and the payment recipient, in some cases the batching and netting of multiple payments, and the establishment of final positions for settlement. *See* COMM. ON PAYMENTS AND MKT. INFRASTRUCTURES, BANK FOR INT'L SETTLEMENTS, DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENT, CLEARING AND SETTLEMENT 10

model are described in further detail below.

A. Platform Services

Services in the first layer of the payment stack—consumer platform services—enable individual consumers, through physical devices or software, to initiate a payment transaction and to access funds or credit in their payment accounts, in the third layer of the payment stack.[40] Physical payment cards—credit, debit, and prepaid cards—have been for many years the most popular consumer platforms for paying for goods and services in the United States. Payment cards include credit cards (providing access to revolving credit accounts), debit cards (providing access to funds in bank accounts), and prepaid cards (providing access to funds previously provided to the issuer but without a permanent account).[41]

Today, wallet services offered through Apple Pay, PayPal, Venmo, and Zelle also allow consumers to store payment account information—the details from physical payment cards, bank and other account information, or, increasingly, randomly generated numbers (or "tokens") that replace those details—in a payment "wallet."[42] These wallet services are used either to pay merchants for goods and services or to make person-to-person payments.[43]

To pay for goods or services, a consumer initiates a transaction on a consumer platform, which communicates with a processing service

---

(2017) [hereinafter BIS/CPMI, LEDGER TECHNOLOGY], https://www.bis.org/cpmi/publ/d157.pdf [https://perma.cc/6N6Y-3CQL]. Settlement occurs once the ledger of the settlement service provider is updated and the recipient's service provider is credited. *See* Mills et al., *supra* note 9, at 5–7, 13.

40. *See* GOV'T ACCOUNTABILITY OFFICE, GAO-17-361, FINANCIAL TECHNOLOGY: INFORMATION ON SUBSECTORS AND REGULATORY OVERSIGHT 18–19 (2017), https://www.gao.gov/assets/690/684187.pdf [https://perma.cc/A2PU-6VLD]; EVANS & SCHMALENSEE, *supra* note 18, at 157.

41. *See* MANN, *supra* note 16, at 11, 61, 79.

42. *See, e.g.*, *Apple Pay Security and Privacy Overview*, APPLE, https://support.apple.com/en-us/HT203027 [https://perma.cc/D8JR-N46R] (explaining that, when using Apple Pay, "your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple"); Peter Rudegeair, *Why Apple and J.P. Morgan Are Chasing Venmo*, WALL ST. J. (June 26, 2017, 5:30 AM), https://www.wsj.com/articles/why-apple-and-j-p-morgan-are-chasing-venmo-1498469401 (describing competition among wallet providers such as Apple Pay, Venmo, PayPal, and Zelle).

43. *See* MARIANNE CROWE ET AL., FED. RESERVE BANK OF ATLANTA & FED. RESERVE BANK OF BOS., IS PAYMENT TOKENIZATION READY FOR PRIMETIME? 9 & n.20 (2015), https://www.bostonfed.org/-/media/Documents/PaymentStrategies/tokenization-prime-time.pdf [https://perma.cc/JUM3-UKDD].

provider in the second layer of the payment stack that has contracted with the merchant to assist in receiving payments.[44] To initiate an in-person transaction, a consumer swipes the magnetic strip or inserts the chip of a payment card, or uses contactless technology embedded within a payment card or mobile phone.[45]

For an internet or other remote transaction—where the consumer is not physically present at the merchant's store—a consumer inputs the details of the payment card or relies on previously stored payment details in a payment wallet.[46] For some mobile and internet transactions, such as those involving ride-sharing services like Uber and Lyft, there is no distinct moment of payment because logging into the platform serves as authorization for any goods or services ordered on it.[47] In that way, digital wallets have made the mechanics of payments less visible to consumers.[48]

The consumer platform and merchant processor usually work together to encrypt the payment details or replace sensitive payment card information at the time of payment initiation with dynamically-created tokens.[49] The platforms then submit the payment details or token to a processing service provider in the second layer of the payment stack, without any further involvement, except to receive a notification as to whether the transaction was successful.[50]

B. Processing Services

Because digital payments require an enormous amount of technical expertise and computing storage and processing capacity,[51] most merchants as well as most payment providers in other payment stack

---

44. *See* First Data Corp., Annual Report (Form 10-K) 7–8 (Feb. 24, 2017) [hereinafter First Data Corp., Form 10-K], https://investor.firstdata.com/~/media/Files/F/FirstData-IR/documents/2016-form-10-k.pdf.

45. *See, e.g.*, *id.* at 4, 7–8 (describing the general methods for conducting in-person payment card, internet, and mobile transactions).

46. *See id.*

47. *See* WORLD ECON. FORUM, BEYOND FINTECH: A PRAGMATIC ASSESSMENT OF DISRUPTIVE POTENTIAL IN FINANCIAL SERVICES 36–39 (2017), http://www3.weforum.org/docs/Beyond_Fintech_-_A_Pragmatic_Assessment_of_Disruptive_Potential_in_Financial_Services.pdf.

48. *See id.*

49. *See* CROWE ET AL., *supra* note 43, at 16 (describing the tokenization process in the context of mobile wallets).

50. *See Dwolla Terms of Service*, DWOLLA (Jan. 14, 2016), https://www.dwolla.com/legal/tos/ [https://perma.cc/U6RV-LTB4] (explaining that Dwolla's partner banks carry out the remainder of the transaction process using messaging and settlement services).

51. *See* FIN. STABILITY BD., *supra* note 1, at 1, 19, 27, 30.

layers contract with third-parties that provide a broad range of payment-related "back-end" processing services.[52] Even in circumstances where companies provide services to both consumers and businesses, it is the business that typically pays for the processing service, with the processor acting as the agent or affiliate of an account service provider in the third layer of the payment stack or as the agent of a merchant.[53]

Processing services include merchant processors, which enable merchants to receive payments by offering software, hardware, and processing services that allow merchants to communicate with consumer platforms in the first layer and accept internet payments or in-person payments.[54] They also include services to payment account providers in the third layer of the payment stack, sending and receiving payment messages on their behalf to other layers of the payment stack, including messaging networks and settlement systems,[55] and managing customer billing and other communications.[56]

Some companies, including PayPal, Square,[57] and Dwolla,[58] provide both consumer platform services and business processing services. Other merchant processors, including incumbents, like First Data, Vantiv,[59] and Authorize.net (a Visa subsidiary),[60] and newer entrants, like Braintree (a PayPal subsidiary)[61] and Alkami,[62] focus on the merchant side of the

---

52. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK: RETAIL PAYMENT SYSTEMS 19–20 (2016) [hereinafter FFIEC, IT EXAMINATION HANDBOOK], https://ithandbook.ffiec.gov/media/274860/ffiec_itbooklet_retailpaymentsystems.pdf [https://perma.cc/2NBQ-D8ZG].

53. *See infra* Section III.C.1 (describing the exceptions to money transmitter regulation). Dwolla, for example, operates as an agent of its partner banks, allowing it to operate, for regulatory purposes, as a platform service, rather than an account service. *See About Our Financial Institution Partners*, DWOLLA, https://www.dwolla.com/legal/about-our-financial-institution-partner/ [https://perma.cc/E7EB-TG4S] (last visited Oct. 2, 2018).

54. *See, e.g.*, Square, Inc., Annual Report (Form 10-K) 4 (Feb. 24, 2017) [hereinafter Square, Form 10-K], https://s21.q4cdn.com/114365585/files/doc_financials/2016/q4/Square_10K_2016.pdf.

55. *See Debit and Credit Card Processing Solutions*, FIRST DATA, https://www.firstdata.com/en_us/products/global-and-national-financial-institutions/credit-and-debit-processing-solutions.html [https://perma.cc/QA4X-GVBN] (last visited Oct. 2, 2018); *Credit and Debit Card Solutions*, FIRST DATA, https://www.firstdata.com/en_us/products/merchants/card-and-check-acceptance.html [https://perma.cc/VG74-Q7PT] (last visited Oct. 2, 2018).

56. *See Customer Communications Solutions*, FIRST DATA, https://www.firstdata.com/en_us/products/global-and-national-financial-institutions/customer-communications-solutions.html [https://perma.cc/AM68-CTER] (last visited Oct. 2, 2018).

57. *See* Square, Form 10-K, *supra* note 54, at 4.

58. *See Dwolla Terms of Service*, DWOLLA, (Jan. 14, 2016), https://www.dwolla.com/legal/tos/ [https://perma.cc/CL47-6B8N].

59. *See* EVANS & SCHMALENSEE, *supra* note 18, at 157.

60. *How Payments Work*, AUTHORIZE.NET, https://www.authorize.net/resources/how-payments-work/ [https://perma.cc/JW2Y-2QXV] (last visited Oct. 2, 2018).

61. *Get Started – Overview*, BRAINTREE, https://articles.braintreepayments.com/get-

transaction. Still others serve niche payments markets, such as payments platform and processing for particular types of merchants.[63]

Companies need not specialize in payment services to provide vital infrastructure to the payments ecosystem. Financial services generally, and payment services in particular, are increasingly dependent on large technology companies to provide important informational technology infrastructure.[64] Cloud service providers such as Amazon Web Services,[65] Microsoft Azure,[66] and Google Cloud Platform[67] provide data storage and processing infrastructure and cybersecurity and business continuity services to payments companies in all layers of the payment stack. These cloud platforms also provide access to ecosystems of data management and analytic services, including artificial intelligence and customer data collection and analysis services, supplied by software companies like IBM[68] and Salesforce.[69]

By outsourcing these resource-intensive technology services, account providers and merchants can focus on implementing their core business models.[70] As part of a larger trend to outsource technology-related functions in financial services, all but the largest banks are increasingly

started/overview [https://perma.cc/GK2S-DNTT] (last visited Oct. 2, 2018).

62. *Solutions – Intuition Meets Innovation*, ALKAMI, https://www.alkami.com/features [https://perma.cc/T6BN-DAW3] (last visited Oct. 2, 2018); Katie Roof, *Alkami Raises $70 Million for Mobile Banking Software*, TECHCRUNCH (Jan. 9, 2018), https://techcrunch.com/2018/01/09/alkami-raises-70-million-for-mobile-banking-software/ [https://perma.cc/77T8-6GKK].

63. *See, e.g.*, *Message from the CEO*, AFFINIPAY, https://affinipay.com/about/ [https://perma.cc/W252-66XM] (last visited Oct. 2, 2018).

64. WORLD ECON. FORUM, *supra* note 47, at 27 ("Financial institutions of all sizes are increasingly dependent on large techs' cloud□based infrastructure to scale and deploy processes and to harness artificial intelligence (AI) as a service.").

65. *See Banking & Payments*, AMAZON WEB SERVICES, https://aws.amazon.com/financial-services/banking/ [https://perma.cc/8N34-TB4Q] (last visited Oct. 2, 2018).

66. *See Azure SaaS Applications for Financial Services*, MICROSOFT AZURE, https://azure.microsoft.com/en-us/industries/financial/ [https://perma.cc/Z882-XNCX] (last visited Oct. 2, 2018).

67. *See Financial Services Solutions*, GOOGLE CLOUD, https://cloud.google.com/solutions/financial-services/ [https://perma.cc/V67M-C8TV] (last visited Oct. 2, 2018).

68. *Front Office Banking Is Leading Modernization of the Financial Services Industry*, IBM, https://www.ibm.com/industries/banking-financial-markets/front-office/ [https://perma.cc/8RT7-WY4H] (last visited Oct. 2, 2018).

69. *See CRM 101: What is CRM*?, SALESFORCE, https://www.salesforce.com/crm/what-is-crm/ [https://perma.cc/5Y7P-2SYC] (last visited Oct. 2, 2018).

70. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, RISK MANAGEMENT OF OUTSOURCED TECHNOLOGY SERVICES 1 (2000), https://www.federalreserve.gov/boarddocs/srletters/2000/sr0017a1.pdf [https://perma.cc/ZQN3-RASH] ("[O]utsourcing to affiliated or nonaffiliated entities can help financial institutions manage costs, obtain necessary expertise, expand customer product offerings, and improve services . . . .").

outsourcing processing activities to nonbanks.[71] Banks generally outsource these services when specialized companies have a comparative advantage due to expertise or economies of scale.[72] This can reduce operating costs and avoid large, fixed-cost investments in processing technology.[73]

C. Account Services

The third layer of the payment stack consists of payment account services that are provided directly to consumers and businesses, allowing them to use a deposit or other account to fund or receive payments. Consumers access their payment accounts through a consumer platform service in the first layer of the payment stack; merchants and other businesses access their accounts through a processing service in the second layer. Payment account providers rely on connection services in the fourth layer of the payment stack to connect to the underlying payments infrastructure, messaging and settlement services in the fifth and sixth layers. Payment account holders can use their accounts to make either retail or wholesale payments, as described in further detail below.

1. Retail Payment Accounts

Consumers can make retail payments from three basic types of accounts: deposit or other demand accounts, revolving credit lines, and prepaid balances. Payments from these accounts are made through payment card transactions, automated clearing house ("ACH") transactions, or retail real-time payment ("Retail RTP") transactions.

A typical payment card transaction involves two account service providers. The first provider, an issuer, provides consumers with a physical card or other payment device and commits to withdraw funds from the purchaser's account (in the case of a debit or prepaid card) or to otherwise pay for the transaction (in the case of a credit card).[74] The second provider, an acquirer, acting on behalf of the merchant, collects

---

71. *See, e.g.*, BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 1 (noting "the trend for banks to outsource payments and technology-related services"); *id.* at 15 ("Although banks have outsourced specific back-end payment functions to non-banks for some time, increased competition and new technology have recently created more scope for such outsourcing.").

72. *See id.* at 15.

73. *See id.*

74. MANN, *supra* note 16, at 11.

payments from the issuer.[75] As described in more detail below, payment card messaging services enable the issuers and acquirers to communicate and to calculate daily net balances owed to one another, while actual settlement takes place in a separate transaction using a settlement service in the sixth layer of the payment stack.

ACH began as a method to make recurring payments such as utility bill payments and payroll deposits,[76] but has more recently become an important payment method for the purchase of goods and services, especially over the internet,[77] with the rise of PayPal and other nonbank payment account providers.[78] It is by far the largest system for relatively low-dollar payments, processing more than 23 billion transactions worth over $145 trillion in payments annually.[79] ACH payment transactions are typically completed within one or two business days.

Retail RTP service, introduced in the United States in 2017, is primarily intended to provide U.S. banks and their account holders with a faster, near real-time method of conducting payments that would otherwise go through the slower ACH process.[80] Its speed may also lead to expansion into payments that have been traditionally processed using wholesale real-time payment services, such as just-in-time inventory and other supplier payments, as well as some goods and services purchases over the internet.[81]

Banks have historically dominated the payment account market because of their built-in relationships with customers who can use their existing checking or other demand accounts to make payments, but nonbanks today also allow their customers to conduct payment card, ACH, and RTP transactions.[82] A nonbank account provider such as PayPal and Venmo aggregates its customer accounts in a pooled account held at a bank and must ultimately connect to messaging and settlement

---

75. *See id.*

76. *See id.* at 88.

77. *See* FFIEC, IT EXAMINATION HANDBOOK, *supra* note 52, at 15–16.

78. *See* PAYPAL, PAYFLOW ACH PAYMENT SERVICE GUIDE 12, 25 (2013), https://www.paypalobjects.com/webstatic/en_US/developer/docs/pdf/pp_achpayment_guide.pdf [https://perma.cc/CP9B-9H5X]. For transactions over the internet, PayPal's account services allow merchants to initiate debits from the customer's bank account using ACH. *See id.* at 25.

79. FED. RESERVE BD., *supra* note 4, at 2.

80. *See RTP: Sample Use Cases,* CLEARING HOUSE, https://www.theclearinghouse.org/payment-systems/-/media/0785f93ee3534695b445dbc42a310b90.ashx [https://perma.cc/BV7W-F7DD] (last visited Oct. 2, 2018).

81. *See id.*

82. *See, e.g.*, First Data Corp., Form 10-K, *supra* note 44, at 4, 7 (describing the general methods for conducting such internet and mobile transactions).

service providers through that bank's connection services.[83]

Nonbanks whose core business is payments—like American Express, MoneyGram, PayPal, Square, Stripe, TransferWise, Venmo, and Western Union—provide payment account services, as do larger, more diversified nonbank companies like Google and Facebook,[84] online merchants like Amazon, and sharing economy platforms like Airbnb.[85] Nonbank account service providers earn money by investing the balances of customer accounts, earning interest or other returns.[86] They may also provide account services in order to facilitate other aspects of their business. Airbnb, for example, provides account services and holds a guest's payment in the guest's account—a form of escrow—until after the transaction is complete.[87]

2. Wholesale Payment Accounts

Wholesale payment services (also known as large-value payment services) allow banks to conduct payments on their own behalf or on behalf of their account holders.[88] These account holders include banks that do not have direct access to wholesale payment systems (including foreign banks), nonbank financial service providers holding pooled accounts for their own customers, commercial businesses, and individual consumers.[89] Most of the payments made using wholesale payment

83. Richard J. Sullivan, *The Federal Reserve's Reduced Role in Retail Payments: Implications for Efficiency and Risk*, ECON. REV., 3d Quarter 2012, at 79, 85–86, https://www.kansascityfed.org/PUBLICAT/ECONREV/PDF/12q3Sullivan.pdf [https://perma.cc/EG3X-8RT5].

84. *See, e.g.*, *Directory of Money Transmitters*, CAL. DEP'T BUS. OVERSIGHT, http://www.dbo.ca.gov/Licensees/money_transmitters/money_transmitters_directory.asp [https://perma.cc/64TJ-X8ZH] (last visited Oct. 2, 2018) (listing these companies as licensed money transmitters under California law).

85. *See, e.g.*, *id.*

86. *See, e.g.*, *Paypal User Agreement: About Your Account*, PAYPAL, https://www.paypal.com/us/webapps/mpp/ua/useragreement-full [https://perma.cc/4HUK-4GDQ] (last visited Oct. 2, 2018) ("PayPal combines your PayPal balance with the PayPal balances of other PayPal customers and invests those funds in liquid investments in accordance with state money transmitter laws. PayPal owns the interest or other earnings on these investments.").

87. *See* FED. TRADE COMM'N, THE "SHARING" ECONOMY: ISSUES FACING PLATFORMS, PARTICIPANTS, AND REGULATORS 48 (2016), https://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf [https://perma.cc/6EE6-E9VE].

88. FED. FIN. INSTS. EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 207 (2014) [hereinafter FFIEC BSA/AML EXAMINATION MANUAL], https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf [https://perma.cc/D658-QP7J].

89. *See id.* at 207–08 & 208 n.203; MANN, *supra* note 16, at 213; *FSOC Annual Report*, 2012 Fin. Stability Oversight Council 146 [hereinafter *FSOC Ann. Rep.*], https://www.treasury.gov/initiatives/fsoc/Documents/2012%20Annual%20Report.pdf [https://perma.cc/L3E2-YF5T].

accounts—payments related to interbank loans, real estate transactions, or other financial market transactions—are time-sensitive and high in value.[90] Transactions using these systems are discussed in more detail below in Sections II.E.2 and II.F.2.

D. Connection Services

Only banks with a commercial presence in the United States may access U.S. messaging and settlement services in the fourth and fifth layers of the payment stack. Nonbanks providing payment account services to consumers or businesses must as a result maintain their own accounts at banks to complete payment transactions.[91] Connections to banks may also allow nonbank platform, account, and processing service providers to provide value-added services such as pass-through deposit insurance on funds held in their accounts.[92] Foreign banks without a branch or subsidiary in the United States may access U.S. messaging and settlement services, either by opening an account at a correspondent bank (a U.S. bank that provides certain services to foreign banks) or by relying on cross-border arrangements that the Federal Reserve Banks have established with a limited number of other countries.[93]

If a foreign bank has a correspondent account with a U.S. bank, it can use that account to make payments on its own behalf or on behalf of its customers and to conduct other financial activities in the United States.[94] To complete some cross-border transactions, a chain of correspondent banks in multiple countries may be required, often resulting in the assessment of multiple fees, which are generally passed on to end-users.[95]

The Federal Reserve Banks also provide connection services that

---

90. *See FSOC Ann. Rep.*, *supra* note 89, at 146. This Article classifies Fedwire as a wholesale payment system although one-third of Fedwire payments are less than $5,000. *See* Sullivan, *supra* note 83, at 82.

91. *See, e.g.*, THE CLEARING HOUSE PAYMENTS CO. L.L.C., CHIPS RULES AND ADMINISTRATIVE PROCEDURES 25–26 (2013) [hereinafter CHIPS RULES], https://www.theclearinghouse.org/~/media/files/payco%20files/rulesgov%202013%20(3).pdf?la=en [https://perma.cc/FPU5-K985]; THE CLEARING HOUSE PAYMENTS CO. L.L.C., ELECTRONIC PAYMENTS NETWORK: RULES OF MEMBERSHIP AND OPERATING RULES 2 (2016); 12 C.F.R. 210.25–210.32 (2018) (setting out operating rules for banks that participate in Fedwire).

92. *See, e.g.*, *Digital Currency Balances*, COINBASE, https://www.coinbase.com/legal/insurance [https://perma.cc/2ARR-AEUA] (last visited Oct. 2, 2018).

93. *See* Heath Tarbert & Liangshun Quian, *The Perils and Promise of Correspondent Banking*, 133 BANKING L.J. 53, 53 (2016).

94. *See id.* at 55. "Payable-through" correspondent accounts allow account holders to conduct payments and other banking activities directly on their own behalf. *See* 31 C.F.R. § 561.307 (2017).

95. *See* FASTER PAYMENTS TASK FORCE, *supra* note 3, at 28.

allow U.S. banks (and their customers) to send and receive cross-border payments. FedACH facilitates international ACH payments by creating connections with either a depository institution or a central bank-operated transfer network in another country.[96] The service is currently limited to Canada, Mexico, Panama, and most European countries.[97]

E. Messaging Services

The service suppliers in the first four layers allow consumers, merchants, and other businesses to access funds and credit lines, leveraging the specialized resources of technology, logistics, and operations companies, and relying on banks to connect them to the underlying payments infrastructure. That infrastructure—consisting of messaging and settlement services—is what allows those connecting banks to communicate with one another and ultimately to transfer funds among themselves.

Messaging services are responsible for the flow of payment instructions sent among the banks involved in a payment transaction. The payment instructions sent using messaging services enable the authorization and clearing of payment transactions and, in some cases, communicate the settlement instructions to be carried out by settlement service providers in the sixth layer of the payment stack, but they do not carry out the actual transfer or settlement of funds.[98]

1. Retail Payment Messages

There are three types of messaging services that relay messages among banks involved in retail payment transactions. Retail messaging services of the first type—consumer payment card networks—process the vast majority of payments that consumers and business make in exchange for goods and services in the United States—more than 100 billion transactions worth nearly $6 trillion.[99] They send messages for

---

96. *See* FED. RESERVE BD., REPORT TO THE CONGRESS ON THE USE OF THE AUTOMATED CLEARINGHOUSE SYSTEM FOR REMITTANCE TRANSFERS TO FOREIGN COUNTRIES 9, 14–16 (2011), https://www.federalreserve.gov/boarddocs/rptcongress/ACH_report_201107.pdf [https://perma.cc/DCZ7-NYEG]; *see also* GOV'T ACCOUNTABILITY OFFICE, *supra* note 2, at 42.

97. FED. RESERVE FIN. SERVS., FEDGLOBAL ACH PAYMENTS SERVICE ORIGINATION MANUAL 11 (2016), https://www.frbservices.org/assets/financial-services/ach/global-service-orig-manual.pdf [https://perma.cc/TDV4-6VHW].

98. *See* MANN, *supra* note 16, at 224–25.

99. *See* FASTER PAYMENTS TASK FORCE, *supra* note 3, at 53; FED. RESERVE BD., *supra* note 4, at 2.

transactions initiated through physical payment cards (credit, debit, and prepaid) and wallets loaded with payment card details.[100]

Modern payment cards began in the mid-twentieth century as end-to-end services, with one company acting as the sole intermediary between a consumer and a merchant in a payment transaction. These early payment card operations were generally regional operations: consumer banking was at the time disaggregated into regional fiefdoms, and because of the end-to-end nature of the service, cardholders were generally able to use their cards only at merchants that shared the same bank.[101] That changed when the corporate predecessors to Visa and Mastercard began to operate national "interchanges" enabling cardholders to use their cards outside their bank's region of operation.[102]

The chief function of the interchanges was—and still is—to transfer information about a transaction between the cardholder's issuing bank and the merchant's acquiring bank.[103] The brand names of network operators like American Express, Discover, Mastercard, Visa, and the STAR Network are well-known to consumers, because their logos appear on payment cards in consumer pockets, even though the services are provided to banks.[104]

Payment card networks play two key roles in payment card transactions. Their first role is to facilitate the authorization of a payment card transaction.[105] When a purchaser uses a payment card to pay, the merchant platform initiates payment submission by sending a message to the merchant's bank or a processing service provider, which then routes the transaction information to a payment network.[106] The payment network contacts the consumer's bank and assists that bank in verifying the cardholder's information, conducting fraud detection analyses, and determining whether the cardholder has sufficient funds or credit.[107] If the transaction is approved, the network sends an approval message back to the merchant's bank or the processing provider, as well

---

100. *See* MANN, *supra* note 16, at 79.

101. *See* LEWIS MANDELL, THE CREDIT CARD INDUSTRY: A HISTORY 31 (1990).

102. *See id.*

103. *See id.*

104. *See* SUSAN HERBST-MURPHY, CLEARING AND SETTLEMENT OF INTERBANK CARD TRANSACTIONS 4 (2013), https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf [https://perma.cc/P9A2-NQ9W]; First Data Corp., Form 10-K, *supra* note 44, at 13 (noting that Visa, Mastercard, Discover, and the STAR Network compete for debit card network services).

105. *See* FASTER PAYMENTS TASK FORCE, *supra* note 3, at 53.

106. *See* First Data Corp., Form 10-K, *supra* note 44, at 7–8.

107. *See id.*

as the merchant, through the merchant platform.[108]

The second role of the payment card networks is to facilitate the clearing and settlement steps of a transaction through a separate series of messages. At the end of each day, a merchant submits a batch of its approved authorizations to an account service provider or a processing service provider.[109] The account provider or processor then routes the batch to the payment card network, which sorts the transactions attributed to each consumer bank and merchant bank, and provides summaries of the net financial positions to each participant.[110] The network does not itself settle the transaction but submits a fund transfer order to a settlement system.[111]

Messaging services of the second type, ACH messaging services, perform similar functions in a payment transaction, although they batch together many transactions, at the end of each day or another set time period, for authorization and clearing.[112] There are two leading providers of ACH messaging services. The Federal Reserve operates FedACH, which began as an extension of the Federal Reserve Banks' traditional clearinghouse function for paper checks,[113] a function required by statute.[114] The Clearing House Payments Company—a private consortium of large banks—competes with FedACH to provide ACH services through its Electronic Payments Network ("EPN").[115] In recent years, the Federal Reserve and EPN have roughly split the ACH market in the United States, each with approximately 50% market share.[116]

The third type of retail messaging services, retail RTP messaging

---

108. *See id.*

109. *See id.*

110. *See id.*

111. *See id.*; MANN, *supra* note 16, at 17, 64.

112. Unlike payment card transactions, which are authorized on an individual basis, an ACH operator batches and nets payment messages at the end of a set time period (usually one or two days) before routing payment instructions for authorization. *See* MANN, *supra* note 16, at 90–92. And instead of settlement occurring in a separate transaction at the end of each day as in a payment card transaction, ACH authorization occurs at the same time that the payment is settled among participating banks. *See* PAYPAL, *supra* note 78, at 12, 25.

113. *See* Mark Edwin Burge, *Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law*, 67 HASTINGS L.J. 1493, 1513 (2016).

114. *See* 12 U.S.C. § 360 (2012) ("Every Federal reserve bank shall receive on deposit at par from depository institutions or from Federal reserve banks checks and . . . drafts drawn upon any of its depositors . . . .").

115. GOV'T ACCOUNTABILITY OFFICE, *supra* note 2, at 8–9, 36. The 1980 Monetary Control Act requires that the Federal Reserve charge fees for its services based on all direct and indirect costs actually incurred in providing its services and imputed costs, taking into account costs that would have been incurred by a private company. 12 U.S.C. § 248a (2012).

116. GOV'T ACCOUNTABILITY OFFICE, *supra* note 2, at 47.

services, send messages regarding each step of the payment transaction so that the transaction is completed in near real-time, without batching or netting to reduce transaction volume as in ACH and payment card transactions.[117] Both The Clearing House RTP system and the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") provide retail RTP messaging services.[118] Since 2017, The Clearing House's RTP system has supported real-time or near real-time payments in amounts up to $25,000.[119] The system relies on technology developed by Vocalink, a Mastercard subsidiary that also operates RTP services in other countries, including the United Kingdom.[120] SWIFT is a Belgium-headquartered cooperative of thousands of banks founded in 1977,[121] and has until recently focused its U.S. offerings on wholesale payment messaging services.[122]

2. Wholesale Payment Messages

Wholesale payment messages are typically sent using one of three messaging services. The Federal Reserve has operated the first service, the Fedwire Funds Service, since 1918, to conduct transfers that are immediate, final, and irrevocable among U.S. banks that maintain accounts at a Federal Reserve Bank.[123] The Clearing House, a consortium of about 50 of the largest U.S. banks, operates the second service, The Clearing House Interbank Payment System ("CHIPS").[124]

---

117. *See* THE CLEARING HOUSE PAYMENTS CO. L.L.C., REAL-TIME PAYMENTS OPERATING RULES 29–30 (2017) [hereinafter REAL-TIME PAYMENTS OPERATING RULES], https://www.theclearinghouse.org/payment-systems/real-time-payments/-/media/6de51d50713841539e7b38b91fe262d1.ashx [https://perma.cc/6CJK-D78F].

118. *SWIFT to Facilitate Instant Payments in the U.S.*, SWIFT (Aug. 15, 2017), https://www.swift.com/news-events/press-releases/swift-to-facilitate-instant-payments-in-the-u_s_ [https://perma.cc/5FRQ-D5AQ].

119. *First New Core Payments System in the U.S. in More Than 40 Years Initiates First Live Payments*, CLEARING HOUSE (Nov. 14, 2017) [hereinafter *First New Core Payments System*], https://www.theclearinghouse.org/payment-systems/articles/2017/11/20171114-rtp-first-new-core-payments-system [https://perma.cc/B3S3-3PM2]; REAL-TIME PAYMENTS OPERATING RULES, *supra* note 117, at 14.

120. *See First New Core Payments System*, *supra* note 119.

121. *SWIFT History*, SWIFT, https://www.swift.com/about-us/history [https://perma.cc/A2P3-TUGF] (last visited Oct. 2, 2018).

122. *See* COMM. ON PAYMENT AND SETTLEMENT SYS., BANK FOR INT'L SETTLEMENTS, THE INTERDEPENDENCIES OF PAYMENT AND SETTLEMENT SYSTEMS 25 (2008), https://www.bis.org/cpmi/publ/d84.pdf [https://perma.cc/SM7P-MUNT] (describing SWIFT messaging services).

123. *See* MANN, *supra* note 16, at 213, 226.

124. THE CLEARING HOUSE, CHIPS PARTICIPANTS (2018) https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/chips_participants_revised_05-29-2018.pdf [https://perma.cc/J9YN-MGEQ] (listing 45 direct participants as of May 29, 2018); *see also* MANN,

Fedwire and CHIPS provide both messaging and settlement services to participants, facilitating the authorization, clearing, and settlement steps of a transaction without the need for a separate messaging provider.[125] The messages contain not only authorization instructions or net values for settlement but also the instructions to complete settlement.[126] Section II.E.2 provides additional detail on Fedwire and CHIPS.

SWIFT also provides wholesale payment messaging services for settlement on the CHIPS system and for bilateral settlement on the ledger of a correspondent bank at which both the sender and recipient of a payment maintain accounts.[127] In the United States, SWIFT is primarily responsible for sending and receiving information for the U.S. dollar-side of cross-border wholesale payments.[128] Prospective competition from new entrants[129] has spurred SWIFT to roll out its own major upgrade called Global Payments Innovation, which allows a bank's corporate customers to make cross-border payments in a matter of hours and to track the progress of transactions in real-time.[130]

F. Settlement Services

The first five layers in the payment stack do not result in the actual discharge of payment obligations, or settlement, between a payment sender and recipient.[131] That discharge of obligations is generally carried out on networks that facilitate settlement on the ledgers and accounts of a settlement institution, either a private commercial bank or a Federal Reserve Bank.[132] Settlement may occur on a gross basis, so that each transfer is settled individually, or on a net basis, so that credits and debits are periodically offset against each other and the actual volume of

---

supra note 16, at 213.

125. *See* FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 88, at 207–208.

126. *See id.*

127. *See id.* at 209.

128. *See generally SWIFT History*, *supra* note 121.

129. These new entrants include RippleNet. *See* Matthew Leising & Edward Robinson, *Ripple Wants XRP to Be Bitcoin for Banks. If Only the Banks Wanted It*, BLOOMBERG (Jan. 25, 2018, 4:01 AM). Ripple also offers a cross-border payments technology based on DLT, but the adoption rates for the DLT offering are even lower than those for RippleNet. *See id.*

130. *See Major Global Transaction Banks Are Live with SWIFT GPI*, SWIFT (Feb. 16, 2017), https://www.swift.com/news-events/press-releases/major-global-transaction-banks-are-live-with-swift-gpi [https://perma.cc/4KP3-233G].

131. *See* MICHAEL S. BARR ET AL., FINANCIAL REGULATION: LAW AND POLICY 773 (2016).

132. *See* FASTER PAYMENTS TASK FORCE, *supra* note 6, at 22.

transfers is reduced by the offset.[133]

1. Retail Payment Settlement

Two retail payment providers offer both messaging and settlement services: FedACH and The Clearing House's Retail RTP system. The FedACH system provides its own settlement service through accounts at Federal Reserve banks.[134] The Clearing House's Retail RTP system provides settlement together with other steps of a payment transaction, once it has determined that the payment sender has sufficient funds in its pre-funded account.[135]

Three providers offer retail payment messaging services but not their own settlement services: the payment card networks, The Clearing House's ACH offering, and SWIFT's Retail RTP offering. Transactions that rely on the first two for messaging services are settled on the Federal Reserve's settlement systems. Payment card transactions are settled primarily over Fedwire, with some use of FedACH,[136] while payments using The Clearing House's ACH service are settled on the National Settlement Service, which the Federal Reserve Banks operate to provide Fedwire-like settlement services to messaging service providers.[137] SWIFT facilitates transactions that are settled on The Clearing House's RTP system.

2. Wholesale Payment Settlement

Two providers provide wholesale settlement services: Fedwire and CHIPS, which together ultimately settle the vast majority of the value of U.S. dollar payments in the United States—$1,200 trillion annually.[138] In a Fedwire transaction, the participating institution making the payment must either have sufficient funds in its account at the local Federal Reserve Bank or permission under Federal Reserve rules to fund a transfer that would cause its account balance to go temporarily below zero (a circumstance known as a "daylight overdraft").[139] The payments are settled on a gross, immediate, and irrevocable basis during the

133. *See* BARR ET AL., *supra* note 131, at 773.

134. *See* MANN, *supra* note 16, at 88.

135. *See* REAL-TIME PAYMENTS OPERATING RULES, *supra* note 117, at 29–30.

136. *See* HERBST-MURPHY, *supra* note 104, at 12 & n.25 (referring to the use of Fedwire for settlement of Mastercard transactions).

137. *See* FFIEC, IT EXAMINATION HANDBOOK, *supra* note 52, at 14.

138. *See* FASTER PAYMENTS TASK FORCE, *supra* note 3, at 52 & 62 n.63.

139. *See* MANN, *supra* note 16, at 226–27.

systems' week-day operating hours.[140] Fees are charged to both participants, primarily based on the volume of transfers and a fixed monthly participation fee.[141]

CHIPS operates much in the same way as Fedwire, except that it requires participants to maintain a pre-funded account at the Federal Reserve Bank of New York;[142] settles transactions immediately when available balances permit or by the end of the day when the funding account has insufficient funds at the time of the transaction;[143] and at the clearing stage, engages in bilateral and multilateral netting to reduce the actual volume of funds transferred and the amount of funds that participants need to settle payments.[144] Any participant with a net negative position at the end of the day must transfer funds through Fedwire to its CHIPS account.[145]

G. End-to-End Services

The final category in the payment stack model, situated alongside the other six in a parallel track, consists of "end-to-end" providers. These are also known as closed-loop providers because they each provide end-users with the capability to perform all steps in a payment transaction without requiring connections to other payment providers.[146] They maintain direct relationships—usually in the form of accounts—with both the sender and recipient of a payment.[147] The settlement process in particular is simplified because a single provider can settle payments with credits and debits across accounts on its own ledger.[148]

End-to-end payment providers have supplied payment services for

---

140. *See id.*

141. *See, e.g.*, FED. RESERVE BD., THE FEDWIRE FUNDS SERVICE 10 (2014), https://www.federalreserve.gov/paymentsystems/files/fedfunds_coreprinciples.pdf [https://perma.cc/TYW5-T9QW].

142. *See* MANN, *supra* note 16, at 225.

143. *See id.* at 225–26.

144. THE CLEARING HOUSE PAYMENTS CO. L.L.C., CLEARING HOUSE INTERBANK PAYMENTS SYSTEM ("CHIPS") 32–33 (2016), https://www.theclearinghouse.org/-/media/files/payco%20files/standards%20self%20assessment%202016.pdf?la=en [https://perma.cc/2A87-DD7U].

145. COMM. ON PAYMENT & SETTLEMENT SYS., BANK FOR INT'L SETTLEMENTS, PAYMENT AND SETTLEMENT SYSTEMS IN SELECTED COUNTRIES 445 (2003), https://www.bis.org/cpmi/publ/d53.pdf [https://perma.cc/54RN-WP7F].

146. *See* BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 9.

147. *See id.*

148. *See* COMM. ON PAYMENT AND MKT. INFRASTRUCTURE, BANK OF INT'L SETTLEMENTS, FAST PAYMENTS – ENHANCING THE SPEED AND AVAILABILITY OF RETAIL PAYMENTS 16 (2016) [hereinafter BIS/CPMI, FAST PAYMENTS], https://www.bis.org/cpmi/publ/d154.pdf [https://perma.cc/W6QM-PWW3].

many decades. Western Union, which had consolidated the telegraph industry in the United States by the mid-1860s, began to offer end-to-end payment services in the 1870s.[149] A sender could deposit money with a Western Union office in one location, and the telegraph system would transmit payment instructions to another Western Union office, where the recipient could pick up the money.[150] Western Union and its main U.S. competitor, MoneyGram, continue to operate significant end-to-end operations, especially in the cross-border remittance market.[151] The first universal payment cards also began as end-to-end services, with a single company acting as a trusted intermediary between a consumer and a merchant, issuing credit to one and ensuring payment to the other.[152] Over the years other end-to-end payment card operators have appeared, but they represent only a small share of the overall payments market.[153]

Many nonbank payment companies, including PayPal and Venmo, structure their person-to-person payment services as end-to-end services that require both the sender and the recipient of a payment to open an account in order to send or receive money.[154] New end-to-end solutions also promise to improve cross-border retail payments, especially person-to-person payments known as "remittances," transfers made primarily for family, personal, or household purposes.[155] This is a market with relatively significant frictions, making it highly susceptible to change. Cross-border payments take longer to complete than domestic

149. *See* EVANS & SCHMALENSEE, *supra* note 18, at 202.

150. *See id.*

151. Zacks Equity Research, *MoneyGram, Ant Financial Terminate Merger: What's Next*, NASDAQ (January 3, 2018, 9:29 AM), http://www.nasdaq.com/article/moneygram-ant-financial-terminate-merger-whats-next-cm899569; Jaime Toplin, *Legacy Remittance Players Excel in Digital*, BUS. INSIDER (Nov. 6, 2017, 11:39 AM), http://www.businessinsider.com/western-union-moneygram-remittance-players-excel-in-digital-2017-11 [https://perma.cc/M2LG-QZBQ].

152. *See* MANDELL, *supra* note 101, at xiii, 2–3, 157.

153. In 1949, Diners Club began to operate the first universal payment card system. *See id.* American Express began its end-to-end payment card operation in 1987 with its Optima card, with credit supplied directly from American Express. *See id.* at 157; *see also* RONALD J. MANN, ELECTRONIC COMMERCE 707 (2011) (noting that the Discover card also began as an end-to-end service).

154. *See* Sullivan, *supra* note 83, at 86–87.

155. Cross-border payments in retail transactions (other than remittances) remain a small subset of the cross-border market because most major retailers have operations and websites that are specific to each country in which they operate. *See* MANN, supra note 16, at 119. The cross-border retail transactions that do occur are processed by the five largest payment card messaging networks: Visa, Mastercard, American Express, China's UnionPay, and Japan's JCB. *See id.* at 119–20. But cross-border retail transactions, where the merchant does not have retail operations in the country of the consumer, may grow substantially as digital trade activity increases. COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, BANK FOR INT'L SETTLEMENTS, CROSS-BORDER RETAIL PAYMENTS 1, 3 (2018) [hereinafter BIS/CPMI, CROSS-BORDER RETAIL PAYMENTS], https://www.bis.org/cpmi/publ/d173.pdf [https://perma.cc/NZ23-6QER].

transactions,[156] and costs associated with remittances have been "notoriously high," with a global average cost of ten percent in 2008.[157] Those costs have declined more than two percent in less than ten years,[158] as new entrants and incumbents alike have introduced faster and cheaper ways to transfer money overseas,[159] without using traditional end-to-end remittance providers, such as Western Union,[160] or payment services that rely on correspondent banks or other cross-border connection services.[161]

Aside from remittances and other person-to-person payments, however, end-to-end payment providers play a relatively small role in the payments marketplace, although new entrants have been successful in some markets, such as Kenya and India, with relatively little competition from incumbent payment providers.[162]

III. REGULATION ACROSS THE PAYMENT STACK

The payment stack model constructed in Part II shows that payment services sort into categories according to the function that they serve in payment transactions. This Part describes the regulatory objectives in payment services—consumer protection, law enforcement, and financial stability—as they map onto each layer of the payment stack. Figure 2 provides a summary of that mapping.

---

156. *See* BIS/CPMI, CROSS-BORDER RETAIL PAYMENTS, *supra* note 155, at 1.

157. *See* DONG HE ET AL., INT'L MONETARY FUND, VIRTUAL CURRENCIES AND BEYOND 21–22 (2016), https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf [https://perma.cc/WTH4-UXMN].

158. *See* The World Bank, *An Analysis of Trends in Cost of Remittance Services*, Remittance Prices Worldwide, Sept. 2017, at 1, https://remittanceprices.worldbank.org/sites/default/files/rpw_report_september_2017.pdf [https://perma.cc/WAP8-685P]; DONG HE ET AL., *supra* note 157, at 21–22.

159. New entrants like TransferWise and CurrencyFair offer cheaper exchange rates by directly matching buyers and sellers of different currencies, without relying on third-party intermediaries like bank currency exchangers. *See* Houman B. Shadab, *Financial Technology*, *in* REFRAMING FINANCIAL REGULATION: ENHANCING STABILITY AND PROTECTING CONSUMERS 416, 425 (Hester Peirce & Benjamin Klutsey eds., 2016), https://www.mercatus.org/system/files/peirce_reframing_web_v1.pdf [https://perma.cc/YTL7-UG2V]. TransferWise has been doubling in size each year and now handles more than $1 billion in payments each month. Martin Arnold, *Financial Industry Faces Extreme Disruption in Payments*, FIN. TIMES (Sept. 26, 2016), https://www.ft.com/content/1b82a0e6-4f67-11e6-8172-e39ecd3b86fc. Incumbent players are also getting involved. Barclays in the UK and the Commonwealth Bank of Australia plan to allow customers to send payments between the two countries using only a phone number. *Id.*

160. *See supra* Section II.G.

161. *See supra* Section II.D.

162. *See* BIS/CPMI, FAST PAYMENTS, *supra* note 148, at 11 n.10, 22 (citing examples in Kenya and India, among others).

SERVICE LAYER	REGULATORY OBJECTIVES		
	CONSUMER PROTECTION	LAW ENFORCEMENT	FINANCIAL STABILITY
PLATFORM	*narrow*		
PROCESSING			*derivative*
ACCOUNT	YES	YES	
CONNECTION	*background bank regulation*		
MESSAGING		*narrow*	
SETTLEMENT			YES

Figure 2: Regulation of Payment Stack Layers

The model shows that regulators have largely taken a functional approach to their treatment of these services, so that services within each payment stack layer are subject to the same type of regulation. As described in the following sections, the core aspects of payments regulation are neutral as to technology and business model. Consumer protection rules—including a risk allocation regime for unauthorized transactions and surety bond requirements for money transmitters—attach to account providers because those providers contract directly with consumers and hold funds on their behalf. Law enforcement rules, including customer due diligence and suspicious transaction reporting requirements, attach to account providers as well because those providers have primary access to customer information. And measures supportive of financial stability, including the application of enhanced prudential standards to systemically important financial market utilities and the government operation of infrastructure, enhance certainty in the actual transfer of funds among banks.

The model also shows that what we think of payments regulation is today primarily concerned with the activities within only two of the six payment stack layers: account and settlement services. Other payment services are generally not subject to payment-specific regulation, with some modest exceptions. This is partly because account and settlement services are the ones that may pose payment-specific risks and partly because regulators may not need to impose payments-specific regulation on activities that are already subject to derivative and background banking regulation. The following sections describe the scope and nature of regulation in each payment stack layer.

A. Platform Services

Most providers of consumer platform services—although they interact with consumers and allow them to initiate payment transactions—do not maintain a contractual relationship with those consumers. They instead supply their services to providers of processing and account services in the second and third layers of the payment stack. Largely for that reason, no federal law or regulation specifically governs consumer platform services.[163]

B. Processing Services

U.S. financial regulators regulate processing services—a field dominated by nonbanks—only when they are provided to banks and, even then, only maintain a derivative supervisory relationship with processing service providers as part of their oversight of those banks. When nonbanks enter into contractual arrangements with banks, regulators are authorized to supervise the supply of those services to banks, primarily for operational and related risks that their operations may pose to the financial stability of the banks.[164] Regulators continue to evaluate risk management primarily through examination of the banks themselves,[165] which in turn impose private contractual requirements in the form of vendor management programs on their nonbank service providers.[166]

---

163. Payment providers, including consumer platforms in the first layer of the payment stack, fall outside the reach of federal consumer protection rules, for example, if they: (1) do not hold customer accounts; and (2) provide their services according to contractual arrangements with banks that issue payment cards or with other account-holding institutions. *See* 12 C.F.R. § 1005.14 (2018). Basic state and federal consumer financial protection rules, including the federal Consumer Financial Protection Act of 2010, which disciplines "unfair, deceptive, or abusive acts" in connection with consumer financial products and services, do apply to the relatively few platform services that are provided directly to consumers. *See* 12 U.S.C. § 5531 (2012); *see also* In the Matter of Dwolla, Inc., Consent Order CFPB No. 2016-CFPB-0007 (Mar. 2, 2016) (identifying and imposing remedies with respect to compliance with these federal consumer protection rules).

164. *See* 12 U.S.C. §§ 1464, 1867, 5514(e), 5515(d), 5516(e) (2012).

165. *See* Div. of Banking Supervision & Regulation & Div. of Consumer & Cmty. Affairs, Fed. Reserve Bd., Guidance on Managing Outsourcing Risk 2 (2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf [https://perma.cc/8DH5-WD3D] ("The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations.").

166. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS 1 (2012) [hereinafter FFIEC, SUPERVISION OF TSPS], https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf [https://perma.cc/8FDW-RCHN] ("The Agencies expect financial institutions to have a comprehensive, enterprise risk management process in place that addresses vendor management for their relationships with

The Bank Services Company Act, for example, authorizes the three federal banking regulators—the Federal Reserve, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency—to examine and regulate certain payment services provided on behalf of or to federally insured banks.[167] The Federal Deposit Insurance Act also authorizes those regulators to take enforcement actions against "institution-affiliated parties," which may include nonbank processing providers, that have engaged in knowing or reckless conduct that "caused or is likely to cause more than a minimal financial loss to, or a significant adverse effect on, the insured depository institution."[168] Analogous state laws authorize state banking regulators to supervise nonbank processing providers that contract with state-licensed banks.[169]

The federal banking regulators coordinate their supervision of processing service providers through the Federal Financial Institutions Examination Council ("FFIEC"),[170] in consultation with state banking regulators.[171] Consistent with the role of this layer in the payment ecosystem, the examinations focus on identifying and mitigating risks associated with a provider's information technology services.[172]

C. Account Services

The regulatory focus in the account services layer of the payment stack is on consumer protection and law enforcement objectives. Even though banks serve as the ultimate custodians of nonbanks' pooled

---

[technology service providers ('TSPs')]").

167. *See* 12 U.S.C. § 1867 (2012); *see also* GOV'T ACCOUNTABILITY OFFICE, FINANCIAL TECHNOLOGY 26 (2017), https://www.gao.gov/assets/690/684187.pdf [https://perma.cc/9UP7-UZB4].

168. *See* 12 U.S.C. § 1813(u)(4) (2012).

169. *See, e.g.*, N.Y. COMP. CODES R. & REGS. tit. 23, § 500.11 (2018).

170. *See* FFIEC, SUPERVISION OF TSPS, *supra* note 166, at 4 ("The Agencies coordinate the interagency programs for the supervision of TSPs through the FFIEC. The programs establish responsibilities and requirements for the collaborative efforts of the Agencies to ensure effective supervision while making efficient use of examiner resources and reducing burden on the TSPs.").

171. *See FFIEC State Liaison Committee (SLC)*, FED. FIN. INSTS. EXAMINATION COUNCIL, https://www.ffiec.gov/slc.htm [https://perma.cc/V8T2-UZC5] (last modified Sept. 22, 2017, 11:43 AM).

172. *See* FFIEC, SUPERVISION OF TSPS, *supra* note 166, at 1 ("The Agencies conduct IT-related examinations of financial institutions and their TSPs based on the guidelines contained in the IT Handbook."). Although not enforced by regulators, private-system rules such as the NACHA rules that govern ACH transactions also impose risk-management controls on financial institutions that choose to rely on third-party service providers. *See* FFIEC, IT EXAMINATION HANDBOOK, *supra* note 52, at 52.

accounts, the banks and nonbanks in this layer are subject to the same general type of consumer protection and law enforcement regulation because the nonbanks maintain pooled accounts on behalf of their customers.

1. Consumer Protection

Account services provided to consumers are subject to consumer protection laws and regulations, at both the federal and state level.

a. Federal Regulation

The most important federal consumer protection rules are those that govern the allocation of losses internal to individual consumer transactions and provide incentives to account service providers to ensure that they process only transactions that have been authorized by their customers.[173] These rules allocate nearly all risk of losses due to unauthorized transactions to the banks that issue credit cards to consumers (under the Truth in Lending Act ("TILA") and Regulation Z)[174] or to entities that enable payments using funds held in payment

173. Federal law and regulation also apply rules governing consumer disclosures and statements, the issuance of access devices, methods for resolving errors, and overdrafts to account service providers. *See, e.g.*, 15 U.S.C. §§ 6801–6809 (2012) (providing disclosure and customer consent rules with respect to the sharing of nonpublic personal information about consumers with unaffiliated third-parties under the Gramm-Leach-Bliley Act); 15 U.S.C. §§ 1601–1667f (2012) (providing consumer disclosure, error resolution, overdraft, and other rules for consumer credit card transactions under the Truth in Lending Act); 12 C.F.R. §§ 1026.1–.61 (2018) (same); 15 U.S.C. §§ 1693–1693r (2012) (providing consumer disclosure, error resolution, and other rules for consumer account transactions under the Electronic Funds Transfer Act); 12 C.F.R. §§ 1005.1–.36 (2018) (same). The Gramm-Leach-Bliley Act allows disclosures to nonaffiliated companies, including service providers in the other layers of the payment stack in a number of circumstances, including arrangements that are disclosed to the consumer. *See* 15 U.S.C. § 6802(b)(2), (e). Federal law and regulation also grant credit card users the right to refuse payment to the issuing bank if the goods or services are unsatisfactory or not delivered, subject to certain conditions and restrictions. *See* 15 U.S.C. § 1666i(a) (unsatisfactory performance); 15 U.S.C. § 1666(a), (b)(3) (non-performance). Users of all other digital payment methods are not afforded this "chargeback" right. *See* Clayton P. Gillette & Steven D. Walt, *Uniformity and Diversity in Payment Systems*, 83 CHI.-KENT L. REV. 499, 510–11 (2008) (noting that no such rule applies to debit card transactions); James Steven Rogers, *Unification of Payments Law and the Problem of Insolvency Risk in Payment Systems*, 83 CHI.-KENT L. REV. 689, 692 (2008) (same); Ronald J. Mann, *Making Sense of Payments Policy in the Information Age*, 93 GEO. L.J. 633, 640–46 (2005) (noting that no such rule applies to wire transfers and debit card transactions). The distinction is based on historical concerns that consumers making purchases with a credit card may not adequately understand borrowing's negative consequences, although many consumers today use credit cards simply for convenience and pay off their balances in full each month. *See* Mann, *supra* note 173, at 651–52, 656. Reported chargeback rates are in any event extremely low, significantly below one percent. *See id.* at 661.

174. *See* 15 U.S.C. § 1643; 12 C.F.R. § 226.12 (2018); *see also* MANN, *supra* note 16, at 12.

"accounts," including payments using a debit card, prepaid card, ATM, an ACH service, or the Retail RTP service (under the Electronic Funds Transfer Act ("EFTA") and Regulation E).[175] Private contracts between card issuers and other network participants, including merchants, as well as state laws, may re-allocate these risks.[176]

TILA and Regulation Z limit consumer liability for unauthorized transactions (e.g., due to fraud) to $50 in point-of-sale transactions where the issuer provides for some method for the cardholder to identify as the user of the card (e.g., signature or photograph on the card), impose no liability for unauthorized internet transactions and other transactions based solely on card numbers, and require credit card issuers to disclose credit terms and conditions to credit card users. *See* 12 C.F.R. § 226.12; Truth in Lending (Regulation Z), 76 Fed. Reg. 79,768, 79,957–58 (Dec. 22, 2011) (codified at 12 C.F.R. pt. 1026). Under prevailing market norms, however, issuing banks generally waive even the $50 of liability that the statute permits in point-of-sale transactions. *See* MANN, *supra* note 16, at 111. Although an individual cardholder is not generally liable for losses associated with his card, card issuers may have incentives to pass losses onto cardholders as a whole in the form of higher interest rates and fees, subject to market forces to compete on price. *See* L. Ali Khan, *A Theoretical Analysis of Payment Systems*, 60 S.C. L. REV. 425, 464 (2008).

175. *See* 15 U.S.C. §§ 1693–1693r; 12 C.F.R. §§ 205.1–.20 (2018); 12 C.F.R. §§ 1005.1–.36 (2018). EFTA applies only to transfers of funds involving accounts "established primarily for personal, family, or household purposes." 15 U.S.C. § 1693a(2). EFTA and Regulation E do not generally apply to wire transfer systems because those systems are not primarily designed to transfer funds on behalf of individuals. *See* 12 C.F.R. § 205.3(c)(3) (excluding Fedwire and other systems "used primarily for transfers between financial institutions or between businesses"). The Consumer Financial Protection Bureau revised Regulation E in February 2018 (with a proposed effective date of April 2019) to apply EFTA to prepaid cards in most instances. *See* 12 C.F.R. § 1005.2(b)(3) (providing that "prepaid cards" generally fall within EFTA protections); Rules Concerning Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 83 Fed. Reg. 6364, 6420 (Feb. 13, 2018) (to be codified at 12 C.F.R. pt. 1005, 1026) (stating that the term "debit card" generally includes the term "prepaid card" for purposes of EFTA). The key distinction between debit card and prepaid card transactions is that a prepaid card allows access to a balance previously dedicated to the card without the need for a demand deposit account at a financial institution. *See* Liran Haim & Ronald Mann, *Putting Stored-Value Cards in Their Place*, 18 LEWIS & CLARK L. REV. 989, 992 (2014). This may create an additional risk for the consumer in that the issuer of a prepaid card—unlike the issuer of a debit card—need not be a depositary institution with federal deposit insurance, and the consumer is exposed to the risk that the issuer will become insolvent. *See id.* at 1009–10. Together, EFTA and Regulation E generally limit consumer liability for unauthorized transactions to $50 or $500, depending on the circumstances, shifting responsibility in most cases to the originating institution, and require institutions holding consumer accounts to disclose to consumers the terms and conditions that will govern payments made from their accounts. *See* 12 C.F.R. §§ 205.4, 205.6–.7. Consumer liability is technically unlimited under EFTA in extreme circumstances, where the account holder does not report the loss or theft of an access device such as debit card within 60 days, or within a reasonable time in certain extenuating circumstances and the failure to report is a "but for" cause of the account holder's losses. *See* 15 U.S.C. § 1693g(a). By their terms, TILA and EFTA also refer to slightly different concepts of "unauthorized" use, *compare* 15 U.S.C. § 1602(o) (defining "unauthorized use" by reference to a person without "actual, implied, or apparent authority"), *with* 15 U.S.C. § 1693a(12) (defining "unauthorized electronic fund transfer" by reference to a person without "actual authority"), although it is difficult to discern any practical difference, *see* Gillette & Walt, *supra* note 174, at 520 (noting "few reported instances in which consumer liability for third-party use of a credit card has rested on the presence of implied or apparent authority and that would likely have been decided differently had the debit card standard been applied").

176. *See* BARR ET AL., *supra* note 131, at 765.

Although not implicating consumer protection interests, it is useful to note that a parallel risk allocation regime exists for transactions involving non-consumers. For those transactions, the risk of loss is generally allocated through a combination of the rules of the relevant settlement network (if any), Article 4A of the Uniform Commercial Code ("UCC") as implemented in state law, and private contract.[177] The result in most cases is that the account providers—and not their customers—bear the risk of loss.[178]

Allocation of liability—away from the consumer and in most cases away from other customers—increases confidence and participation in

177. *See, e.g.*, Robert G. Ballen & Thomas A. Fox, *The Role of Private Sector Payment Rules and a Proposed Approach for Evaluating Future Changes to Payments Law*, 83 CHI.-KENT L. REV. 937, 938–42 (2008). Fedwire is governed by Regulation J, which largely incorporates the requirements of Article 4A of the UCC, *see* 12 C.F.R. §§ 210.25–210.32 (2018), and Federal Reserve Operating Circular No. 6, *see generally* FED. RESERVE FIN. SERVS., FEDERAL RESERVE BANKS OPERATING CIRCULAR NO. 6 (2017), https://www.frbservices.org/assets/resources/rules-regulations/operating-circular-6-102917.pdf [https://perma.cc/FX4E-PJMD]. The Federal Reserve's related National Settlement Service is similarly governed by Federal Reserve rules and federal and state law. *See generally* FED. RESERVE FIN. SERVS., FEDERAL RESERVE BANK OPERATING CIRCULAR NO. 12 (2016), https://www.frbservices.org/assets/resources/rules-regulations/063016-operating-circular-12.pdf [https://perma.cc/2GWT-VSZV]. CHIPS rules apply the law of New York, including Article 4A, to CHIPS transactions. *See generally* CHIPS RULES, *supra* note 91. Federal Reserve ACH transactions are conducted under rules and guidelines developed by a nonprofit banking trade association, NACHA (formerly the National Automated Clearing House Association). *See generally* NACHA, NACHA OPERATING RULES (2018).

178. For customer-initiated ACH and wire transfers, as between the originator and the originator's bank, Article 4A of the UCC generally places the risk of an unauthorized transaction on the originator's bank unless the bank followed "commercially reasonable" security procedures and the information used to access the procedures did not come from a source in the originator's control. *See* U.C.C. §§ 4A-202, 4A-203 (AM. LAW INST. 2012); *see generally* MANN, *supra* note 16, at 258. Because EFTA and Regulation E exclude wire transfers, *see* 12 C.F.R. § 205.3(c)(3), individual consumers who initiate wire transfers fall under this UCC rule, while their transfers over the ACH system falls under EFTA and Regulation E, *see supra* note 175 and accompanying text. Article 4A places any risk of settlement failure (due to the failure of a participating institution or the network operator to satisfy its obligation) on either the originator's bank (e.g., where the beneficiary's bank becomes insolvent), *see* U.C.C. § 4A-402(c) (AM. LAW INST. 2012); *see also* Rogers, *supra* note 173, at 704–05 (describing this "money back guaranty" rule), or the beneficiary's bank (e.g., where the beneficiary's bank does not wait for settlement to occur before crediting the beneficiary's account with available funds), *see* U.C.C. § 4A-405 cmt. 2 (AM. LAW INST. 2012); *see also* Francis J. Facciolo, *Unauthorized Payment Transactions and Who Should Bear the Losses*, 83 CHI.-KENT. L. REV. 605, 614–15 (2008). For ACH transactions where the purported payee attempts to initiate a withdrawal from the non-bank payee's account ("debit" or "pull" transactions), ACH system rules also place the risk of loss on the originating bank, although the contractual arrangement between the bank and the originator usually shifts that risk to the originator. *See* NACHA, *supra* note 177, at §§ 2.2.2.1, 2.2.3. Article 4A also applies to transactions initiated by the payer's payment provider, but it generally defers with respect to those transactions to network rules that govern the ACH and wire transfer systems. *See* U.C.C. § 4A-107 (AM. LAW INST. 2012). Private contracts exclusively govern the remainder of fund transfer transactions: wire transfer transactions where the purported payee attempts to initiate a withdrawal attempting to debit funds from a non-consumer account. *See* Linda J. Rusch, *Reimagining Payment Systems: Allocation of Risk for Unauthorized Payment Inception*, 83 CHI.-KENT L. REV. 561, 589 (2008).

the system and creates incentives for account providers to ensure the security and accuracy of their systems.[179] This maximizes efficient pre-transaction behavior, especially in the case of highly complex payment services with technologically driven features that are exclusively within the control of account providers and their vendors.[180] Consumers retain enough incentives to take steps within their control to avoid unauthorized transactions because of the time and potential cost in reversing unauthorized charges, doubts that the payment providers will honor their obligations, or potentially even ignorance of the consumer protection rules.[181]

b. State Regulation

While federal consumer protection rules allocate the risk of loss associated with individual transactions, a class of state-level laws seeks to protect consumers from entity-level risks associated with certain payments services. The rules seek to ensure that nonbanks providing "money transmission" services—generally defined as the receipt and transmission to others of customer funds—maintain sufficient liquidity to fulfill payment instructions and the ability to honor the withdrawal of funds from accounts in a timely manner, through liquidity (and in some cases, capital) safeguards.[182] Providers in the account services layer of the payment stack are subject to these rules because they hold funds in

179. *See* Burge, *supra* note 113, at 1517, 1539–40. As with supervision of nonbank processing providers, U.S. financial regulators coordinate their supervision and examination of financial institutions' management of risks associated with payments origination, including authentication controls, through the FFIEC. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 1–6 (2005), https://www.ffiec.gov/pdf/authentication_guidance.pdf [https://perma.cc/5GY3-7ZYH].

180. *See* Mann, *supra* note 173, at 638–39 (arguing that losses are in imposed "almost complete[ly]" on payment service providers because of an "implicit premise that losses in technology-driven systems are most effectively reduced by technological and system-design initiatives that are exclusively within the control of the system operator"); Facciolo, *supra* note 178, at 608 (asserting that such allocation does not apply post-transaction to "unauthorized transactions that could be prevented by an account holder's paying attention to her account and its associated statements").

181. *See* Mann, *supra* note 173, at 638.

182. *See* CONFERENCE OF STATE BANK SUPERVISORS & MONEY TRANSMITTER REGULATORS ASS'N, THE STATE OF STATE MONEY SERVICES BUSINESSES REGULATION AND SUPERVISION 4 (2016) [hereinafter CSBS & MTRA], https://www.csbs.org/sites/default/files/2017-11/State%20of%20State%20MSB%20Regulation%20and%20Supervision%202.pdf [https://perma.cc/3WG9-RVNG]; Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG. 495, 535 (2015) ("Existing state 'money transmitter' and 'money services businesses' licensing and prudential supervision regimes are focused primarily on safety and soundness."); BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 36.

payment accounts on behalf of consumers. By contrast, payment platforms in the first stack layer are generally not regulated as money transmitters even though they assist in transactions that involve the transmission of funds to and from those same accounts. That is because platform providers do not have a contractual relationship with consumers. They instead contract with other entities that do have direct consumer relationships or with merchants or other non-consumer parties. The contractual relationship that a platform maintains could be as the agent of a bank,[183] the agent of a merchant,[184] or the "authorized delegate" of a money transmitter.[185]

Forty-nine states, the District of Columbia, and Puerto Rico have licensing regimes for money transmitters,[186] so engaging in money transmission activities on a nationwide basis requires at least 51 licenses no matter where the company is headquartered or otherwise located.[187] The licenses typically require a money transmitter to hold surety bonds as a source of funds in the event of institutional distress or wrongdoing,[188] maintain permissible investments, satisfy minimum net worth requirements, and submit periodic reports on transmission volume and financial status.[189]

---

183. *See, e.g.*, CAL. FIN. CODE § 2010(d) (Deering, LEXIS through ch. 1-109 & 111–157 of 2018 Reg. Sess.) (excluding from money transmitter regulation any commercial bank or industrial bank whose deposits are FDIC-insured, among other firms).

184. *See, e.g.*, CAL. FIN. CODE §§ 2003(b), 2010(l) (Deering, LEXIS through ch. 1-109 & 111–157 of 2018 Reg. Sess.); N.Y. BANKING LAW §§ 640(10), 641(1) (Consol., LEXIS through 2018 ch. 1–205); N.C. GEN. STAT. § 53-208.44(8) (LEXIS through 2018 Reg. Sess. & 1st Extra Sess.). The consumer's payment to the agent is considered final and, if the intermediary is later unable to pay the merchant, the contract between the intermediary and the merchant governs the dispute. California also exempts mobile and online payments for goods or services from other requirements under its money transmitter rules. CAL. FIN. CODE § 2103(a)(2)(B) (Deering, LEXIS through ch. 1-109 & 111–157 of 2018 Reg. Sess.) (exempting those payments from the requirement to provide a "right to refund" statement).

185. *See, e.g.*, N.C. GEN. STAT. § 53-208.44 (LEXIS through 2018 Reg. Sess. & 1st Extra Sess.); OHIO REV. CODE ANN. §§ 1315.01–02 (LexisNexis, LEXIS through Legis. passed by 132nd Gen. Assemb.); VA. CODE ANN. §§ 6.2-1900, -1911 (LEXIS through 2018 Spec. Sess. of Gen. Assemb.).

186. *See PayPal State Licenses*, PAYPAL, https://www.paypal.com/us/webapps/mpp/licenses [https://perma.cc/JB65-DPW9] (last visited Oct. 2, 2018) (listing the jurisdictions where PayPal is licensed as a money transmitter and the acts governing such licensures). Montana does not require a license for money transmitters. *Money Transmitters*, MONTANA.GOV, https://banking.mt.gov/moneytransmitters [https://perma.cc/T8AV-6GZ5] (last visited Oct. 2, 2018) ("There is currently no legislation from the Montana Division of Banking regulating Money Transmitters. Money Transmitters do not have to be licensed with the Division.").

187. *See, e.g.*, PAYPAL, *supra* note 186.

188. *See* Charles Cooper, *Better Tech Allowing State Regulators to Oversee Non-bank Lenders*, HILL (Mar. 13, 2017, 1:20 PM), http://thehill.com/blogs/pundits-blog/finance/323670-better-tech-allowing-state-regulators-to-oversee-non-bank-lenders [https://perma.cc/K65H-JB7R].

189. CSBS & MTRA, *supra* note 182, at 8 (describing common features of state money

State money transmitter licensing requirements generally do not apply to banks, which are already subject to comprehensive regulation at the state and federal levels.[190] This exception exists largely because the primary objective of banking regulation—to ensure the safety and soundness of individual institutions and the financial system as a whole—also serves to ensure that banks will have the resources necessary to comply with their obligations when providing payment services to account holders and other customers.[191]

The classic example of a money transmitter is Western Union, which in its original form took ownership of customer funds at a physical location, deposited them into a bank account, and then waited for the recipient to collect the funds at another physical location of Western Union or that of an agent.[192] Western Union is a licensed money transmitter, although many of its services are end-to-end, as discussed further in Section III.G, because it conducts its core business of peer-to-peer transfers without relying on other service providers.

Most money transmitters today—like PayPal, Venmo, and Square—of course no longer rely on physical locations but instead require end-users to open digital accounts, accessible by computer or phone, and to receive payments using that account. After resisting these licensing regimes for several years, the first of these new money transmitters, PayPal, eventually acknowledged that it fell within this paradigm and today holds money transmitter licenses in all states that require them.[193]

The state-by-state nature of the money transmitter regime has long drawn criticism, spurring efforts in recent years to reduce overlap. State regulators are in the process of standardizing regulatory rules and enhancing cooperative supervision of multi-state money transmitters as part of a broader commitment to adopt an integrated, fifty-state licensing and supervisory system by 2020.[194] A sizeable majority of state regulators now rely on a uniform "Nationwide Multistate Licensing

---

transmitter rules).

190. Some states exempt only federally licensed banks, not banks licensed in another state. Greg Omer, *Fintech: Internet Banking Across State Borders Triggers Compliance Challenges for State Banks*, THOMPSON COBURN LLP (Jan. 20, 2017), https://www.thompsoncoburn.com/insights/blogs/bank-check/post/2017-01-20/fintech-internet-banking-across-state-borders-triggers-compliance-challenges-for-state-banks [https://perma.cc/EQ83-8A5B].

191. *See* MANN, *supra* note 153, at 735; BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 27.

192. *See* EVANS & SCHMALENSEE, *supra* note 18, at 202–03.

193. *See* Hughes & Middlebrook, *supra* note 182, at 548.

194. See Vision 2020 for Fintech and Non-Bank Regulation, CSBS (Jan. 8, 2018), https://www.csbs.org/vision-2020-fintech-and-non-bank-regulation [https://perma.cc/C2WG-LAN3].

System" ("NMLS") to license nonbank money transmitters.[195] The NMLS seeks to expedite regulatory approvals by automating key elements of the approval process and providing common business activity definitions in applying regulatory rules.[196] The states have also established a taskforce through which they coordinate oversight of multi-state money transmitters.[197]

2. Law Enforcement

Account service providers are also subject to law enforcement rules—primarily at the federal level—that are designed to curb money laundering, terrorism financing, and other unlawful activities. Law enforcement regulations generally attach to this layer of the payment stack because they are designed to apply to companies with primary access to information, especially information on end-users, that has "a high degree of usefulness" in law enforcement activities.[198]

At the core of this regulatory regime is the federal Bank Secrecy Act, which requires all "financial institutions," including banks and state-licensed nonbank money transmitters, to report cash transactions of $10,000 or more, verify the identities of their customers,[199] conduct other customer due diligence activities depending on a customer's risk rating,[200] and file suspicious activity reports whenever they "know[],

195. *See* Cooper, *supra* note 188.

196. CSBS & MTRA, *supra* note 182, at 17–19.

197. *See id.* at 12. Some state banking regulators are also discussing the possibility of a "passporting" regime, which would allow a firm to use regulatory approval from one state as permission to operate in another state. *See* Bryan A. Schneider, *State Regulator to Fintechs: We Hear You*, AM. BANKER (Mar. 27, 2017, 9:30 AM), https://www.americanbanker.com/opinion/state-regulator-to-fintechs-we-hear-you [https://perma.cc/VB2K-X3K4].

A recent trend among a small number of states is to attempt an expansion of existing money transmitter regulations to cover entities beyond those that send and receive money on behalf of their account holders. These expansions mean that in a limited number of circumstances a company may be subject to state money transmitter regulation if it "holds itself out" as a money transmitter, advertises or solicits money transmitter services, *see, e.g.*, TEX. FIN. CODE ANN. § 151.302 (West, Westlaw through 2017 Reg. & 1st called Sess. of 85th Leg.), or has the ability to "instruct" payment, *see, e.g.*, WASH. REV. CODE § 19-230-010(18) (2017) (defining "money transmission"), irrespective of whether it exercises control over consumer funds. This is generally counter to the historical purpose of state money transmitter rules to protect consumer funds while they were in the possession of a money transmitter, which "received" and exercised a certain degree of discretionary control over those funds. *See* Judith E. Rinearson & Jeremy M. McLaughlin, *Money Transmitter Licensing, Generally*, *in* PAYMENT SYSTEMS AND ELECTRONIC FUND TRANSFER GUIDE § 300:210 (2018).

198. *See, e.g.*, 31 U.S.C. § 5311 (2012).

199. *See* 31 U.S.C. §§ 5311–5326 (2012); 31 C.F.R. § 1020.100 (2017).

200. *See* FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 88, at 56–59.

suspect[], or ha[ve] reason to suspect" illegal or terrorist activity.[201] U.S. banks maintaining correspondent accounts for foreign banks must exercise enhanced due diligence when opening and managing those accounts[202] and are subject to additional financial record-keeping and reporting for foreign currency clearing and other transactions.[203]

Federal and state laws also require all state-licensed money transmitters and other nonbank "money transmitting businesses" that accept and transmit funds to comply with state money transmitter licensing requirements and to register with the Financial Crimes Enforcement Network of the U.S. Treasury Department ("FinCEN").[204] Money transmitting businesses that fail to register with FinCEN or obtain a state license, or knowingly transfer funds received from or in support of criminal activity, are subject to criminal penalties under both federal[205] and state law.[206] Companies that serve as agents to money services businesses, including providers of platform and processing services in the first two layers of the payment stack, need not register.[207]

D. Connection Services

The connection services that make up the next layer are not subject to regulation designed specifically to address risks arising from their role

---

201. *See* 31 C.F.R. § 1020.320(a)(2) (2017); *see also* FIN. CRIMES ENF'T NETWORK ET AL., INTERAGENCY INTERPRETIVE GUIDANCE ON PROVIDING BANKING SERVICES TO MONEY SERVICES BUSINESSES OPERATING IN THE UNITED STATES 2 (2005), https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf [https://perma.cc/SV3E-MC5Q] ("With limited exceptions, money services businesses [(now, money transmitting businesses)] are subject to the full range of Bank Secrecy Act regulatory controls, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules, and various other identification and recordkeeping rules.").

202. *See, e.g.*, 31 U.S.C. §§ 5318(i), (j), (k).

203. *See* 31 C.F.R. § 1010.630 (2017).

204. The scope of state money transmission licensing regimes is not in all cases coextensive with the scope of this federal registration requirement. *See* 31 U.S.C. § 5330(a) (2012) (requiring any "money transmitting business," whether or not licensed at the state level, to register with the Secretary of the Treasury); *id.* at § 5330(d) (defining "money transmitting business" as any business that provides "money transmitting or remittance services . . . or any other person who engages as a business in the transmission of funds" and "money transmitting service" as "accepting currency or funds . . . and transmitting the currency or funds"); 31 C.F.R. § 1010.100(a), (ddd) (2017) (defining "accept" and "transmittal").

205. *See* 18 U.S.C. § 1960 (2012); 31 U.S.C. § 5330 (2012).

206. *See, e.g.*, N.Y. BANKING LAW §§ 641, 650 (Consol., LEXIS through 2018 ch. 1–205) (providing for misdemeanor and felony penalties for unlicensed money transmission).

207. *See* 31 C.F.R. § 1022.380(a)(3) (2017); *see also* Determination of Money Services Business Status and Obligations Under the Funds Transfer Recordkeeping Rule, and Request for Regulatory Relief, FinCEN Ruling 2009-R004 (Nov. 19, 2009), https://www.fincen.gov/sites/default/files/administrative_ruling/fin-2009-r004.pdf [https://perma.cc/G9X9-QKC7].

in the payment stack. But the overall regulatory regime governing other layers of the stack nonetheless assumes that connection service providers will provide their services and that they are composed of a particular class of firms—banks.[208]

Banks are subject to regulatory requirements that are markedly different from those applicable to nonbank financial service providers. Banking regulation imposes capital requirements and other prudential requirements on banks that have no close analog in the nonbank world.[209] In exchange, banks serve as the exclusive providers of certain financial services (such as deposit-taking and commercial lending funded from that deposit-taking) and receive exclusive access to messaging and settlement services.[210] This exclusivity allows them to act as gatekeepers with respect to all other market participants, advantaging banks in the provision of services that require seamless connections to those systems and increasing incentives for nonbanks to partner with banks rather than challenge them directly in the provision of those services.

E. Messaging Services

For the most part, U.S. financial regulators do not directly regulate messaging service providers, whose operations are governed primarily by contracts among network participants.[211] The one regulatory regime that applies directly to the messaging networks themselves is a relatively narrow set of law enforcement rules.[212] Payment card networks must establish anti-money laundering compliance programs for the selection and approval of participating banks,[213] to prevent those participants from using the network to facilitate money laundering or the financing of terrorist activities.[214] These requirements are in turn hardwired into network operators' own rules governing network participation.[215]

---

208. *See supra* Section II.D.

209. *See* RICHARD SCOTT CARNELL ET AL., THE LAW OF FINANCIAL INSTITUTIONS 50–51, 55 (5th ed. 2013).

210. *See supra* Section II.D; *see also* BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 17–18.

211. *See* MANN, *supra* note 16, at 12; Burge, *supra* note 113, at 1496.

212. The payment card networks are also subject to rules intended to enhance competition, including reporting requirements (e.g., prohibitions on card exclusivity arrangements) and limits on debit card interchange fees. 15 U.S.C. § 1693o-2 (2012); 12 C.F.R. § 235.1–.10 (2018).

213. 31 C.F.R. §§ 1028.100, .210(a) (2017).

214. 31 C.F.R. § 1028.100(e) (2017). For companies that do not have a federal regulator, including operators of credit card systems, FinCEN has delegated examination authority for BSA compliance for companies to the Internal Revenue Service. 31 C.F.R. § 1010.810(b)(8) (2017).

215. *See, e.g.*, MASTERCARD, MASTERCARD RULES 35 (2018), https://www.mastercard.us/

F. Settlement Services

The orderly settlement of payments, especially wholesale payments given their high value, is essential to achieving one payment-related regulatory objective—financial stability.[216] Because settlement may give rise to financial, operational, and other risks to the participants and the settlement system operator, U.S. regulators operate their own settlement systems and subject private operators of systemically important settlement systems to regulation designed to achieve financial stability objectives.[217]

The operators of the two wholesale payment settlement services in the United States, Fedwire and CHIPS, have taken steps to mitigate these risks.[218] For one, there are no credit exposures within CHIPS, either to the system or its participants, because CHIPS has no obligation to settle queued payments, the system provides no credit to participants, and participants do not extend credit to one another over the system.[219]

Liquidity risks to CHIPS participants remain, however, because payment messages in the queue are not guaranteed to settle, and participants may not receive expected payments.[220] If a participant does not meet its final, end-of-day funding requirements, CHIPS will net and process as many outstanding transactions as possible and then delete any unfunded transactions from the system.[221] Participants expecting to receive those deleted payments must arrange to receive any necessary liquidity outside of CHIPS.[222] Liquidity risk is at its highest when participants have a final, end-of-day expected position that depends on other participants meeting their end-of-day funding requirements.[223] The

---

content/dam/mccom/global/documents/mastercard-rules.pdf [https://perma.cc/94US-WTYA].

216. *See* FASTER PAYMENTS TASK FORCE, *supra* note 6, at 22; FIN. STABILITY BD., *supra* note 1, at 47.

217. *The Federal Reserve's Key Policies for the Provision of Financial Services*, FEDERALRESERVE.GOV, https://www.federalreserve.gov/paymentsystems/pfs_frpaysys.htm [https://perma.cc/G9PL-7695] (last updated Nov. 20, 2008) ("The Congress, responding in part to the breakdown of the check-collection system in the early 1900s, made the Federal Reserve an active participant in the payments system when it established the Federal Reserve in 1913. At that time the Congress envisioned that the Federal Reserve would play a dual role as an operator and a regulator of the payments system.").

218. *See* MANN, *supra* note 16, at 274–75. The same is true of settlement that takes place on the accounts of a single correspondent bank, which occurs only once the recipient bank has satisfied itself that the originating bank is able to fund the transfer. *See id.*

219. *See FSOC Ann. Rep.*, *supra* note 89, at 146–47.

220. *See id.*

221. *See id.*

222. *See id.*

223. *See id.*

failure of one institution to meet its funding requirements or a disruption in the system could lead to liquidity problems spreading among participants and their customers.[224]

CHIPS attempts to mitigate liquidity risk to participants through bilateral and multilateral netting arrangements for payments that are processed in batches, so that an individual institution's credits and debits are offset against one another before CHIPS processes payment batches.[225] This reduces liquidity risk by reducing the amount of funds needed to settle payments.[226] There has been only one instance where a participant failed to meet its final funding requirement, resulting in a failure to settle $7.3 billion in payments.[227]

By contrast, Fedwire guarantees the settlement of payments made on its system, including in some circumstances where a bank has exceeded its daily pre-funded balance (a "daylight overdraft"), and it settles each transaction on a real-time basis, rather than waiting to batch and net certain payments together.[228] This provides substantial commercial benefits to Fedwire participants, especially those engaged in large commercial transactions, because the receipt of funds is irrevocable and verifiable in near real-time.[229]

Fedwire mitigates the resulting credit and liquidity risk through system rules and regulation or by bearing the risk itself. The Federal Reserve establishes daylight overdraft limits specific to each bank and charges a substantial fee to cover them, for example.[230] Even so, the Federal Reserve Banks that provide this intraday credit are exposed to the risk that an institution will become insolvent during the course of day, up to the institution's permitted daylight overdraft amount.[231] Fedwire operations are thus premised on the public sector's provision of credit, converting the liquidity risk otherwise borne by participating institutions into credit risk borne by the Reserve Banks.[232]

Under the Dodd-Frank Act, the Financial Stability Oversight Council ("FSOC") must designate as a systemically important "financial market

---

224. *See id.* at 151.
225. *See* THE CLEARING HOUSE PAYMENTS CO. L.L.C., *supra* note 144, at 32–33.
226. *See id.*
227. *See FSOC Ann. Rep.*, *supra* note 89, at 148.
228. *See* MANN, *supra* note 16, at 274–75.
229. *See id.* at 229–30.
230. *See id.* at 227.
231. *See id.* at 229; BARR ET AL., *supra* note 131, at 776.
232. *See* FED. RESERVE BD., *supra* note 141, at 15; *see also* BARR ET AL., *supra* note 131, at 776.

utility" ("FMU") any entity engaged in payment, clearing, or settlement activity if the Council determines that the failure of or disruption to the functioning of the entity could create, or increase, the risk of significant liquidity or credit problems spreading among financial institutions or markets, thereby threatening the stability of the U.S. financial system.[233] FSOC has designated only one payment service provider, The Clearing House, as a systemically important FMU, because it operates CHIPS.[234]

This designation means that The Clearing House is subject to heightened prudential and supervisory provisions intended to promote robust risk management and safety and soundness under the Federal Reserve Board's Regulation HH,[235] which is based on international risk-management standards for payment services.[236] Regulation HH prescribes standards relating to governance, risk management, and credit risk, including rules requiring The Clearing House to establish a plan for recovery and orderly wind down and to meet minimum capital and liquidity requirements.[237]

Other settlement systems, due to their smaller size or design choices, do not pose the same type or degree of risk. Although ACH services process large sums, multilateral netting and batching at the end of the each day before settlement has largely eliminated credit and liquidity risk.[238] Messaging networks that process payment card transactions, for their part, also engage in multilateral netting, further reducing volumes that are already too small to contribute materially to financial risks

---

233. *See* 12 U.S.C. §§ 5461–72 (2012).

234. Press Release, U.S. Dep't of the Treasury, Financial Stability Oversight Council Makes First Designations in Effort to Protect Against Future Financial Crises (July 18, 2012), https://www.treasury.gov/press-center/press-releases/Pages/tg1645.aspx [https://perma.cc/HP7M-KFYQ] (announcing the designation of The Clearing House Payments Company, "on the basis of its role as operator of the Clearing House Interbank Payments System"); *see also* 12 C.F.R. § 1320.1–.20 (2018) (setting out the process for designation of financial market utilities).

235. *See* 12 C.F.R. § 234.1–.6 (2018); *see also* 12 U.S.C. § 5461 (2012) (authorizing the Federal Reserve to provide enhanced supervision over financial market utilities).

236. *See generally* COMM. ON PAYMENT & SETTLEMENT SYS. & THE TECH. COMM. OF THE INT'L ORG. OF SEC. COMM'NS, BANK FOR INT'L SETTLEMENTS, PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES (2012), https://www.bis.org/cpmi/publ/d101a.pdf [https://perma.cc/DD5R-H9GE].

237. *See* 12 C.F.R. § 234.1–.6. Even settlement systems that are not designated as FMUs are subject to enhanced prudential standards under the Federal Reserve's Policy on Payment System Risk if they are expected to settle a daily aggregate gross value of U.S. dollar-denominated transactions exceeding $5 billion on any day during the next 12 months. *See* Policy on Payment System Risk, 79 Fed. Reg. 2838, 2841 (Jan. 16, 2014). Settlement systems subject to the policy must identify, monitor, and manage general business risk and maintain liquid net assets sufficient to ensure a recovery or orderly wind down of critical operations. *See generally* Policy on Payment System Risk, 79 Fed. Reg. at 2850.

238. *See* Mann, *supra* note 19, at 966–67.

associated with settlement systems.[239] The Clearing House's Retail RTP system does not generally engage in multilateral netting and batching but currently operates at much lower volumes than the other retail services.

G. End-to-End Services

End-to-end payment providers are generally subject to the cumulative range of regulations that apply to the providers of individual services within the payment stack. The primary exception as a practical matter is in the area of remittances. Because this is a market dominated by end-to-end providers, regulation that applies specifically to remittances in practice applies predominantly to those providers.[240] The CFPB issued regulations in 2013 that seek to enhance transparency and accountability of remittance transactions involving U.S. consumers, while also establishing default execution rules for remittance market participants.[241] The rules apply to any supplier that conducts remittance transfers for U.S. persons, whether or not the consumers hold an account with the supplier.[242]

This Part has described the scope and nature of regulation governing the services that make up the payment stack model. The next Part examines a range of potential consequences of financial change on the structure and content of the payment stack model and sets out regulatory strategies for addressing those potential effects.

IV. STRATEGIES FOR ADDRESSING THE POTENTIAL CONSEQUENCES OF FINANCIAL CHANGE ON THE PAYMENT STACK

The model presented in this Article is useful in visualizing two basic concepts: one, that despite the vast array of payment services and providers, both old and new, they sort into a relatively small number of interconnected categories; and two, that despite the smattering of seemingly disparate U.S. payments regulations and regulators, payment services within each category are generally subject to the same types of rules and standards.

---

239. The current volume of retail payments transacted over the payment card messaging networks is an order of magnitude or two smaller than the overall volume of wholesale payments. *See id.* (suggesting that there is "relatively limited systemic need for supervision of the operations" of banks with a primary focus on consumer payments).

240. *See* 12 C.F.R. § 1005.30–.36 (2018).

241. *Id.*

242. 12 C.F.R. §§ 1005.30(f)-(g).

Payments is not a static ecosystem, however, and the payment stack remains subject to market forces, with a wide range of possible outcomes. Markets could fragment and become more decentralized or they could become more concentrated.[243] New entrants could become viable competitors or find themselves swallowed up by incumbents before they become threats.[244] Incumbents that have cultivated consumer trust and brand recognition for decades will at the same time continue to rely on their considerable resources to invest in their own technologies, lower prices as necessary to maintain market share, and acquire their competitors before they present existential challenges.[245]

No matter the outcome of these market forces, a chief lesson from the payment stack model is that the answer to technology or business-model trends is not to engage in a wholesale revision of payments regulation. Instead, the technology-neutral and activity-based nature of payments regulation means that the framework is likely capable of adapting to new challenges, even in times of immense change, and that regulators have the opportunity to follow a more nuanced and tailored approach.[246]

That is not to say that payments regulation should remain static. Financial change is also an opportunity to evaluate areas where new entrants and services underscore existing shortcomings and to examine areas where clarification, substantive revisions, or new approaches would better serve their objectives.[247] And even with a largely technology-neutral and activity-based regulatory regime, financial change may require new regulatory approaches. In some cases, it might cause aspects of regulation to become obsolete, as technology alters the relative importance of various risks, as is possibly the case with the increasingly critical importance of operational risks. In other situations, regulators may be able to affirmatively seek to foster innovation while monitoring financial change that poses relatively low risk.

Change in technology or business model might also provide new, pro-regulatory opportunities.[248] It may allow regulators to improve their

---

243. *See* FIN. STABILITY BD., *supra* note 1, at 10–11, 21.

244. *See id.* at 10–11.

245. *See* Rysman & Schuh, *supra* note 5, at 43.

246. *See supra* Part III.

247. *See* FASTER PAYMENTS TASK FORCE, *supra* note 6, at 39 ("The Faster Payments Task Force asks the Federal Reserve to initiate an effort with relevant regulators to evaluate current laws with respect to faster payments, clarify the applicability of and make appropriate changes to regulations, and promulgate new regulations as needed.").

248. *See* Christopher G. Bradley, *FinTech's Double Edges*, 93 CHI.-KENT L. REV. 61 (2018).

regulatory and supervisory methods, particularly in information collection and analysis. Or it may present regulators with the opportunity to assist in advancing market-based solutions that benefit regulators, service providers, and customers. The following analyzes each of these potential strategies in turn.

A. Expressly Apply Existing Regulation to Financial Change

Because payments regulation is largely technology-neutral and activity-based, regulators have been able to adapt to many changes through application of existing regulations. Examples include circumstances where regulators have determined that making payment services faster—and cheaper—is not expected to heighten or introduce new risks[249] or that the risks associated with payment services do not materially vary depending on whether the transactions are recorded on a distributed ledger.[250] Enhancing legal certainty through explicit application of existing regulation can, where appropriate, promote customer welfare, reduce compliance costs, and mitigate operational risks.[251]

The widespread application of existing state money transmitter and federal anti-money laundering regulation to virtual currency services in the third layer of the payment stack is instructive. Nearly all state and federal regulators have determined that virtual currency wallet and other payment account providers relying on distributed ledger technology ("DLT") pose the same types of financial risks as traditional account service providers because they are responsible for holding value on behalf of their customers.[252] The role of these account providers in DLT transactions has allowed regulators to apply existing money transmission regulations in the account services layer of the payment stack.[253]

Application of existing payments regulation is generally feasible in

---

249. *See* BIS/CPMI, FAST PAYMENTS, *supra* note 148, at 1.

250. *See* BIS/CPMI, LEDGER TECHNOLOGY, *supra* note 39, at 1.

251. *See, e.g.*, FIN. STABILITY BD., *supra* note 1, at 4.

252. *See* Hughes & Middlebrook, *supra* note 182, at 498 ("Intermediaries to cryptocurrency transactions act much like intermediaries to transactions in traditional payment systems. They pose similar types of credit and liquidity risks to consumers, market participants, and national economies. The increasing prevalence of intermediaries in cryptocurrency transactions necessitates regulation of these new market participants."); BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 1–2 (noting that nonbanks and banks do not pose "fundamentally different" risks in retail payment services); GOV'T ACCOUNTABILITY OFFICE, *supra* note 40, at 24 ("Many of the potential risks associated with mobile payments are the same as those that exist with traditional payment products.").

253. *See* DONG HE ET AL., *supra* note 157, at 25–28.

these circumstances because current DLT use cases require account providers to serve as gatekeepers to enter or exit the DLT system. Even an open and permissionless DLT network requires trusted intermediaries to interface with the broader economy, to "cash into" the system to fund virtual currency transactions with an initial infusion of fiat currency, and to "cash out" of the system to pay for goods, services, and investments in fiat money.[254] These gatekeepers will continue to serve these critical functions as long as DLT services continue to operate alongside, rather than in lieu of payments in U.S. dollars.[255] End-users may in any event continue to choose to store their private and public keys required to access and send tokenized money with a wallet or other account provider.[256]

The state-level approach to virtual currencies has not been entirely uniform, but the clear trend is to treat payment services that use virtual currency no differently than payment services transmitting legal tender. Most states that have considered the issue of virtual currency businesses have issued guidance that interprets existing money transmitter rules as encompassing virtual currency activities[257] or modified their laws or regulations to make clear that existing money transmitter regulations apply to virtual currency businesses.[258] Nearly all states have issued licenses under existing money transmitter rules to companies that rely at least in part on virtual currencies.[259]

---

254. *See id.* at 25.

255. Additional complications beyond the scope of this Article may arise with large-scale issuance of non-fiat currency. *See* DONG HE ET AL, *supra* note 157, at 16 (noting monetary policy complications of non-fiat currencies).

256. *See* Hughes & Middlebrook, *supra* note 182, at 497.

257. *See, e.g.*, DIV. OF CONSUMER SERVS., DEP'T OF FIN. INSTS., UNIFORM MONEY SERVICES ACT: INTERIM REGULATORY GUIDANCE (2014), http://dfi.wa.gov/documents/money-transmitters/virtual-currency-interim-guidance.pdf [https://perma.cc/APE3-CF9R].

258. *See, e.g.*, N.C. GEN. STAT. § 53-208.42(20) (LEXIS through 2018 Reg. Sess. & 1st Extra Sess.) (defining "virtual currency" for purposes of the state's money transmittal rules). A small minority of states—including Texas and Kansas—have declined to impose money transmitter regulations directly on virtual currency activities, on the theory that virtual currency is not "money" and has no monetary value. *See, e.g.*, CHARLES G. COOPER, BANKING COMM'R, TEX. DEP'T OF BANKING, SUPERVISORY MEMORANDUM – 1037 (2014), https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf [https://perma.cc/C9WC-EAAZ]; KAN. OFFICE OF THE STATE BANK COMM'R., MT 2014-01, REGULATORY TREATMENT OF VIRTUAL CURRENCIES UNDER THE KANSAS MONEY TRANSMITTER ACT (2014), http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf [https://perma.cc/Z3FV-8CQ7]. But that approach is likely to make little difference to companies engaged in the transfer of virtual currency, as the money transmission rules still apply to anyone—including a typical virtual currency exchange business—that allows customers to exchange virtual currency and fiat money.

259. CSBS & MTRA, *supra* note 182, at 8–9. The Conference of State Bank Supervisors has also developed a non-binding, model framework suggesting that regulation of virtual currencies should follow existing money transmitter rules. CONFERENCE OF STATE BANK SUPERVISORS, STATE

New York is in the small minority of states that have taken different approaches. It has created a specialized money transmitter license for services that rely on virtual currency, presumably because of heightened consumer protection concerns,[260] but the regime is widely regarded as a failure, with few companies receiving or even seeking a license.[261] The "BitLicense" borrows heavily from the state's existing money transmitter licensing regime, while imposing some obligations that do not apply to other money transmitters and that, in some cases, are duplicative of federal consumer protection and anti-money laundering rules.[262] These include minimum capital requirements that go beyond the surety bond requirements applicable under the state's general money transmission rules.[263]

Federal regulators have also generally applied existing anti-money laundering regulations to virtual currency service providers. FinCEN has made clear that it intends to regulate virtual currency activities in a manner equivalent to similar activities conducted using U.S. dollars and other fiat currencies, noting that the definition of "money transmitter" in the statute does not differentiate between legal tender and virtual currencies that are convertible into legal tender.[264] This appears to be based in large part on a judgment that "virtual currency is not different from other financial products and services" because any payment system can be "exploited for money laundering."[265]

REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES 3 (2015), https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf [https://perma.cc/MX9P-XM44]. A small number of these licenses apply only to currency exchange services and consumer accounts holding U.S. dollars, not the holding or transmission of virtual currency. *See Legal – Licenses*, COINBASE, https://www.coinbase.com/legal/licenses?locale=en-US [https://perma.cc/2XTK-GGJS] (last visited Oct. 2, 2018).

260. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.1–.22 (LEXIS through Aug. 24, 2018).

261. *See* Jen Wieczner, *Inside New York's BitLicense Bottleneck: An "Absolute Failure?,"* FORTUNE (May 25, 2018), http://fortune.com/2018/05/25/bitcoin-cryptocurrency-new-york-bitlicense/ [https://perma.cc/9CJY-WEWY].

262. *See* Hughes & Middlebrook, *supra* note 182, at 536–49.

263. *Compare* N.Y. BANKING LAW §§ 640 (Consol., LEXIS through 2018 ch. 1–205), *with* N.Y. COMP. CODES R. & REGS. tit. 23, § 200.1–.22.

264. FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [https://perma.cc/H3TC-XUQ3]. Observers have noted, however, that FinCEN's guidance may apply to virtual currency businesses in certain circumstances in which it does not apply to other businesses. *See* Elijah M. Alper & Katrina Carroll, *Ensuring a Level Playing Field for Federal Virtual Currency Regulation*, FINTECH L. REP., Jan.–Feb. 2016, at 1, 5–10.

265. Jennifer Shasky Calvery, Director, Fin. Crimes Enf't Network, Remarks at Florida International Banks Association Anti-Money Laundering Conference (Feb. 20, 2014), https://www.fincen.gov/sites/default/files/shared/20140220.pdf [https://perma.cc/R2NV-YP4Z].

Unlike entity-level consumer safeguards at the state level or law enforcement rules at the federal level, allocation of risk under federal consumer protection rules may prove more difficult to apply coherently in some cases. The premise of federal consumer protection rules—particularly rules governing allocation of risk—is that payment account providers have control over authorization of a payment transaction, which confirms whether the appropriate end-user authorized the transaction. These rules may make less sense in circumstances—as in "open, permissionless" DLT systems—in which unidentified entities have at least partial control over authorization of a payment transaction.

U.S. regulators have not yet responded in full to these potential issues.[266] In its recent update to consumer protections regulations under EFTA and Regulation E, for example, the CFPB expressly declined to consider the application of those risk-allocation rules to virtual currency.[267] Although payment providers are able to efficiently allocate risk among themselves through private contracts, regulators have not answered whether consumers should, as a matter of law, benefit from the same risk-shifting mechanisms available to them when using non-DLT account services.[268]

B. Correct Existing Asymmetries in Treatment of Technologies and Business Models

Although expressly applying existing payments regulation to

---

266. Many DLT systems also feature irreversible transactions, making compliance with other aspects of federal consumer regulation—including consumer rights to chargebacks on credit card transactions and error resolution—more difficult and in the case of some, especially permissionless systems, technically impossible. *See supra* note 174.

267. *See* Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z), 81 Fed. Reg. 83934, 83978–79 (Nov. 22, 2016) (codified at 12 CFR pt. 1005, 1026) ("The proposed rule did not resolve specific issues with respect to the application of either existing regulations or the proposed rule to virtual currencies and related products . . . . [T]he Bureau reiterates that application of Regulation E and this final rule to such products and services is outside of the scope of this rulemaking. However, . . . the Bureau continues to analyze the nature of products or services tied to virtual currencies."). Article 4A of the U.C.C. (as reflected in state law), which governs allocation of the risk of unauthorized transactions among commercial participants, also assumes that the originating bank has control over security procedures involved in the initial steps of a payment transaction. *See supra* Section III.C.1.

268. Although similar questions as to the rationality of current allocation rules may arise with respect to platform services such as Apple Pay that may have complete control over the initial steps in a payment transaction, including submission and validation, it is clear at least that the consumer does not generally bear risk of unauthorized transactions, while Apple Pay and its partners are able to resolve questions of allocation among themselves through private contract. *Cf.* Burge, *supra* note 113, at 1526 (noting potential shortcomings of the existing risk allocation regime in the case of platform services that exercise primary control over the authorization of some transactions).

financial change will work in many circumstances, regulators should be cautious in applying off-the-shelf any payments regulation that is not neutral with respect to technology and business model. In those cases, financial change may underscore the need—and provide the impetus—for regulatory improvements. Financial change in this way presents an opportunity to examine old rules and standards with the benefit of a fresh perspective. The opportunity is especially relevant to the details of money transmitter rules in certain states that continue to reflect historical concerns associated with older business models and technologies, creating unnecessary heterogeneity among state-level approaches.[269]

As described above in Section III.C.1, state regulators originally designed money transmitter rules to ensure that entities that intermediate funds on behalf of consumers—those that held consumer accounts or exchanged currency, for example—would not become insolvent and leave their customers without the ability to reclaim their money. But in some states these rules appear to rigidly tie those objectives to fixed capital requirements or bonding requirements that do not reflect the actual risk posed by a participant's size or volume of business in the state.[270]

Some state rules also reflect the business methods and technology of the past, which required consumers to initiate money transmissions in-person, at a Western Union office, for example. Many state statutes assume that payment account service providers in the third layer of the payment stack continue to follow this model, by calculating surety bond and minimum net worth rules, for example, based on the number of physical locations in the state.[271] A very limited set of state regulations also place similarly anachronistic restrictions on consumer platforms in the first payment stack layer that contract with money transmitters, requiring some platforms to maintain a physical location in the state.[272]

---

269. *See* Benjamin Lo, *Fatal Fragments: The Effect of Money Transmission Regulation on Payments Innovation*, 18 YALE J.L. & TECH. 111, 117–20 (2016).

270. *See, e.g.*, ME. REV. STAT. ANN. tit. 32, § 6107 (Westlaw through May 2, 2018) (establishing a fixed surety bond amount of $100,000); OHIO REV. CODE ANN. § 1315.04(C)(2) (LexisNexis, LEXIS through Legis. passed by 132nd Gen. Assemb.) (establishing a fixed minimum net worth requirement of $500,000).

271. *See, e.g.*, ARIZ. REV. STAT. ANN. § 6-1205.01 (Westlaw through 1st Spec. & 2d Reg. Sess. 53rd Leg.) (establishing minimum net worth requirements based on the number of physical locations); NEV. REV. STAT. § 671.050 (2017) (establishing minimum surety bond requirements based on the number of physical locations).

272. *See, e.g.*, WASH. ADMIN CODE § 208-690-035(4) (LEXIS through July 5, 2018).

C. Prepare for Potential Regulatory Obsolescence from "Payment Stack Collapse"

Although most analyses have concluded that financial change in payments (or in other financial services, for that matter) does not yet pose compelling financial stability risks,[273] the payment stack model can also usefully illustrate the possible future effects of financial change that would make existing regulation obsolete. Obsolescence might lead to a number of negative consequences, including affording commercial advantages to less regulated entities, encouraging strategic law avoidance or influencing other marketplace behaviors,[274] and encouraging firms to price risk according to inconsistent risk management approaches.[275]

The following sets out two possible trends in financial change that may make existing payments regulation obsolete in certain key respects: (1) the possible emergence of DLT as an underlying technology for payment services and (2) the continued rise of nonbanks. Both trends could collapse distinctions among layers in the payment stack model and create conditions that enable less regulated or unidentifiable entities to dominate the provision of services in those layers, leading to possible regulatory escape and diminished regulatory efficacy.

1. DLT-induced Payment Stack Collapse

The emergence of DLT as an underlying technology for payment services could lead to at least two types of payment stack collapse. The first type would result in DLT collapsing distinctions among the connection, messaging, and settlement layers. The second type would collapse distinctions among those layers as well as the account service layer. Figure 3 illustrates both types of DLT-induced payment stack collapse.

Like physical cash or the historical use of bearer bonds, DLT relies on a tokenized form of money, meaning that users exchange digital representations or "tokens" of money directly without the need for a contemporaneous clearing or settlement process that confirms that the

---

273. *See* DONG HE ET AL., *supra* note 157, at 32 (noting that "no contagion to the wider financial system has thus far been observed" due to disruptions in digital money systems); BIS/CPMI, FAST PAYMENTS, *supra* note 148, at 69 ("Most central banks judge that the influence of this type of [fast payment] system on monetary policy and financial stability is limited for the time being.").

274. *See* Tim Wu, Commentary, *Strategic Law Avoidance Using the Internet: A Short History*, S. CAL. L. REV. POSTSCRIPT, Mar. 2017, at 7, 8.

275. *See* BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 2.

originator has sufficient funds or credit.[276] An institution that issues a DLT token to an end-user deducts the token's value as denominated in U.S. dollars or another currency from the end-user's account at the time of issuance, and the end-user is then free to exchange the instrument to a third-party recipient.[277]

From that point on, the fate of the token is no longer the responsibility of the account service provider, and there is no need to check with the account provider to ensure that an account holder was the one that initiated the payment. In a DLT transaction, an end-user initiates the payment with its private key, which is cryptographically combined with the user's public key and information about the payment such as the amount and the public key of the recipient.[278] The end-user's private key operates as a token because the only question to be answered in transaction processing is whether the token is valid, not whether the holder of the token is authorized to spend it.[279] There is no need for separate account, connection, messaging, and settlement services because the use of tokens eliminates the need to debit the sender's account and credit the recipient's account.

276. *See* INT'L ORG. OF SEC. COMM'NS, IOSCO RESEARCH REPORT ON FINANCIAL TECHNOLOGIES (FINTECH) 51, (Feb. 2017) [hereinafter IOSCO RESEARCH REPORT], https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf [https://perma.cc/G6KQ-TA5G]. Introduced in 2009 as the technology underlying the virtual currency bitcoin, DLT involves a ledger, or database, that is distributed over an at least partially decentralized network of computers that enables network participants to share and retain records. *See* Matthew Swinehart & Merritt Baer, *Those Things You've Heard About Bitcoin: Distinguishing Between Signal and Noise*, 16 GEO. J. INT'L AFF. 144, 146–47 (2015).

277. *See* MANN, *supra* note 16, at 9 (describing the issuance and exchange of tokens generally).

278. Swinehart & Baer, *supra* note 276, at 151–52.

279. *See id.*

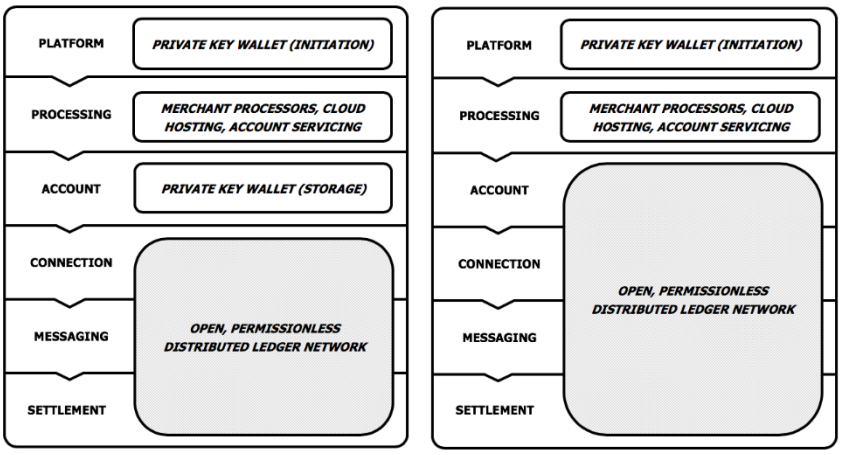

Figure 3: Partial Payment Stack Collapse Due to Nonubiquitous (left) and Ubiquitous (right) Use of Open, Permissionless DLT

a. Open, Permissionless DLT

First-generation DLT regimes such as bitcoin are "open" and "permissionless," meaning that they are accessible by any interested participant,[280] each of which enjoys equal access to the network.[281] Participants may come and go without approval by other participants or a central authority. If open and permissionless DLT regimes become ubiquitous, and there is no need for a user to rely on non-DLT payment services, account providers would become unnecessary and regulators would have no entity to regulate. As shown on the left-hand side of Figure 3, ubiquitous use of DLT payment services could lead to "full" payment stack collapse in the sense that the payment services largely fall outside the existing regulatory perimeter that relies primarily on account providers and settlement systems.

But this "ubiquitous" use scenario would require a degree of virtual currency adoption that appears unlikely based on current evidence. Many first-generation virtual currencies have been the victims of their own success in attracting the public's attention. The volatility and speculative nature of trading in many virtual currencies, for example, has

280. *See* GOV'T ACCOUNTABILITY OFFICE, *supra* note 40, at 41; IOSCO RESEARCH REPORT, *supra* note 276, at 48, 59.

281. *See* Hughes & Middlebrook, *supra* note 182, at 497–98.

made them almost worthless as a payment method.[282] That volatility—and the speculation that drives it—complicates the pricing of goods and services and overloads the system, as those wanting to use virtual currency to make a payment must compete with those wanting to trade it as an asset.[283] Given these realities, it is no surprise that the volume and value of virtual currency transactions remain a tiny fraction of digital payments[284] and that virtual currencies are widely viewed, not as payment methods, but as (rather speculative) investment assets.[285]

And yet a more limited form of payment stack collapse is already the reality with first-generation DLT, as shown in Figure 3. In this "non-ubiquitous" use scenario, account providers such as Coinbase that maintain end-user private keys in a virtual currency wallet, remain identifiable and within the regulatory perimeter because users must cash in and cash out of the DLT system. Banks are no longer needed to provide connection services, however, while the type of financial stability regulation that now attaches at the settlement layer is no longer necessary because no settlement occurs in a tokenized transaction.

b. Closed, Permissioned DLT

The second-generation DLT regimes that may have the most durable promise, including companies like Ripple, are different in many respects from a regulatory perspective. These regimes are "closed" and "permissioned," meaning that the network's nodes are granted access only after meeting certain criteria.[286] This design allows a central authority or existing nodes in a DLT network to grant varying degrees of permission to new participants in terms of access information on the

282. *See* Matt O'Brien, *Bitcoin Is Teaching Libertarians Everything They Don't Know About Economics*, WASH. POST (Jan. 8, 2018) ("Bitcoin changes prices too quickly to be a currency and processes transactions too slowly to be a payments system."); Olga Kharif, *You'd Be Crazy to Actually Spend Bitcoin*, BLOOMBERG (Jan. 4, 2018, 12:00 PM CST), https://www.bloomberg.com/news/articles/2018-01-04/you-d-be-crazy-to-actually-spend-bitcoin.

283. *See* Kharif, *supra* note 282.

284. *See* DONG HE ET AL., *supra* note 157, at 31.

285. *See* Jay Clayton & J. Christopher Giancarlo, *Regulators Are Looking at Cryptocurrency*, WALL ST. J. (Jan. 24, 2018, 6:26 PM), https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363 ("[C]ryptocurrencies are now being promoted, pursued and traded as investment assets, with their purported utility as an efficient medium of exchange being a distant secondary characteristic."); *see also* Paul Vigna & Peter Rudegeair, *MoneyGram Signs Deal to Work with Currency Startup Ripple*, WALL ST. J. (Jan. 11, 2018, 6:34 PM), https://www.wsj.com/articles/moneygram-signs-deal-to-work-with-currency-startup-ripple-1515679285 (noting that only one institution "has signed up to specifically use [Ripple's virtual currency] for settling cross-border trades").

286. *See* Mills et al., *supra* note 9, at 31.

ledger and ability to participate in the consensus mechanism used to validate transactions.[287] Unlike open and permissionless DLT networks, the entities responsible for account services in a second-generation DLT regime remain identifiable and within the existing regulatory perimeter. These regimes are thus unlikely to cause regulatory escape associated with payment stack collapse.

Closed and permissioned DLT regimes are already in limited use in the cross-border wholesale payments market. Incumbent methods of cross-border wholesale payments require a number of intermediaries, each of which adds to the cost of making a payment,[288] and may take up to five days, even for the most common currency pairings.[289] New entrants such as Ripple and Kalypton,[290] as well as a partnership between incumbent Visa and startup Chain, Inc.,[291] promise faster and cheaper cross-border wholesale payments using DLT services.[292]

2. Nonbank-induced Payment Stack Collapse

A second form of payment stack collapse could occur as nonbanks become ubiquitous suppliers of services and supplant banks from the payments market. Because of the historically bank-centric nature of payment services and regulation, displacement of banks could lead to regulatory escape and reduced effectiveness of the existing payment regulatory framework.

The rise of nonbanks in financial services is a trend that is much broader than the payments market. Online and mobile banking has undercut the traditional advantages of physical distribution that banks and their physical retail branches (and later their network of ATMs) once enjoyed.[293] Consumers today are more open to relationships with

287. *See id.*

288. *See id.*, at 18.

289. MCKINSEY & CO., GLOBAL PAYMENTS 2015: A HEALTHY INDUSTRY CONFRONTS DISRUPTION 23–24 (2015), https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-2015-a-healthy-industry-confronts-disruption [https://perma.cc/9E4Z-XS8Q] (follow "Download the report" hyperlink).

290. *See, e.g.*, FASTER PAYMENTS TASK FORCE, *supra* note 3, at 49–50.

291. Eric Sibbitt et al., *Blockchain and Financial Services: Hype or Herald*, 134 BANKING L.J. 208, 208 (2017).

292. *See* Jessie Cheng & Benjamin Geva, *Understanding Block Chain and Distributed Financial Technology: New Rails for Payments and an Analysis of Article 4A of the UCC*, BUS. L. TODAY, March 2016, at 1, 2–3.

293. *See* Dietz et al., *Cutting Through the Noise Around Financial Technology*, MCKINSEY & CO., (Feb. 2016), https://www.mckinsey.com/industries/financial-services/our-insights/cutting-through-the-noise-around-financial-technology [https://perma.cc/X9JU-A8L2].

nontraditional companies that provide personalized and streamlined platform and account services.[294] And nonbank companies have introduced cheaper, more efficient, and more secure processing services, greatly expanding their market share with reliance on improved and expanded data sources, cloud computing and mobile internet functionality, and data analytics, including artificial intelligence and search engine services.[295] Banks increasingly face the choice of competing or partnering with less regulated technology companies, while attempting to maintain their core value proposition.[296]

When it comes to payment services in particular, nonbanks already have a substantial presence. Significant portions of payments and other financial data is now stored and processed using the cloud computing services of large technology companies, including Amazon, Google, and Microsoft.[297] Other technology companies, including Alibaba, Apple, and Facebook have entered the payments market in recent years.[298] And much of modern payments technology, including artificial intelligence and other advanced fraud detection services, depend on access to nonbank services.[299]

The resulting increase in competition from these changes in technology and business models has already placed downward pressure on prices.[300] Other effects are possible in the future, although there is not yet any evidence of regulatory-significant effects in today's market. Nonbank competition may eventually transform payment services from relatively lucrative activities in their own right to loss-leaders for other financial services, or cause payment providers to seek new ways of monetizing relationships with payments customers.[301] Increased competition may mean that banks lose significant revenue from payment services and an anchoring or entry point to other bank services,[302] and in response choose to take on more risk, potentially without proper

294. *See id*.

295. *See* WORLD ECON. FORUM, THE COMPLEX REGULATORY LANDSCAPE FOR FINTECH 9 (2016), http://www3.weforum.org/docs/WEF_The_Complex_Regulatory_Landscape_for_FinTech_290816.pdf [https://perma.cc/REM5-6FLJ].

296. *See* WORLD ECON. FORUM, *supra* note 47, at 28.

297. *See* Martin Arnold, *Finance Chiefs Warn on Big Tech's Shift to Banking*, FIN. TIMES (Feb. 4, 2018), https://www.ft.com/content/d9b3d79e-0995-11e8-8eb7-42f857ea9f09.

298. *See id.*

299. *See id.*

300. *See* BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 19.

301. *See* WORLD ECON. FORUM, *supra* note 47, at 54, 57.

302. *See* DONG HE ET AL., *supra* note 157, at 32 & n.50 (considering the case of digital money); *See* BIS/CPMI, FAST PAYMENTS, *supra* note 148, at 26.

pricing.[303] If nonbanks became dominant in the provision of account services to consumers, for example, there is a possibility that banks would also have reduced access to stable and secure funding from deposits.[304] This could lead to reliance on riskier deposits or wholesale funding, leading to a deterioration in key regulatory metrics such as the net stable funding ratio.[305]

The competitive effects associated with nonbank dominance in the supply of payments services could in turn produce two basic scenarios of payment stack collapse. The first would involve significant displacement of banks from the platform, processing, and account layers of the payment stack, as shown on the left-hand side of Figure 4. This could give rise to questions about the efficacy of the existing regime, particularly with respect to the derivative regulation of nonbank processing services. This scenario is already a reality in some other markets, including China, where technology firms Alibaba and Tencent now control 97% of the payments markets.[306]

The second payment stack collapse scenario would involve displacement of banks further down in the payment stack, including in the connection services layer, as shown on the right-hand side of Figure 4. This would raise more complex questions about the degree to which the background banking regulation applicable to connection services supports financial stability and other regulatory objectives specifically associated with payment services.

But the second scenario would require significant market changes to occur and regulators to grant nonbanks access to the messaging and settlement networks, which are currently available only to banks, reducing or eliminating demand for connection services. As discussed earlier, the bank-centric nature of existing payment services is a function of both the relationships that banks maintain with commercial and

303. FIN. STABILITY BD, *supra* note 1, at 23.

304. *See id.* at 54.

305. Even without a transition to a full or partial payment stack collapse, technological innovations may result in a different mix of financial and operational risks. Where innovations offer faster settlement times, some forms of liquidity risk may be alleviated, at least from the perspective of the recipient institution whose account is credited sooner, but participants must ensure that the availability of their liquidity mechanisms matches any extended operational time. *See* BIS/CPMI, FAST PAYMENTS, *supra* note 148, at 49, 69. Or settlement systems that operate continuously and in real-time may exacerbate bank runs caused by other forces of instability without the benefit of the natural cooling-off periods that the weekly downtime of incumbent settlement systems might provide. *See id.* at 48, 54.

306. He Wei, *Retailers Must Learn to Coexist with Tech Giants*, CHINA DAILY (July 12, 2018, 9:14 AM), http://www.chinadaily.com.cn/a/201807/12/WS5b46ab70a310796df4df5f3c.html [https://perma.cc/8NRS-6URV].

investment banking clients, which account for most of the payments volume (through wholesale regimes), and regulation and system rules that limit participation in messaging and settlement networks.

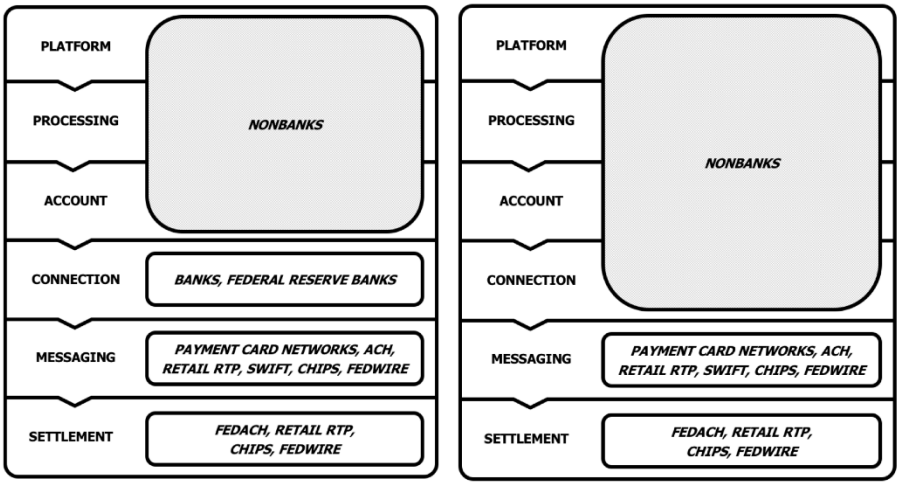

Figure 4: Partial Payment Stack Collapse Due to Dominant Supply by Nonbanks of Services in the Top Three Layers (left) and Top Four Layers (right)

Under either scenario, if nonbanks continue to increase their share of the payments market, regulators could face at least two key challenges related to the bank-centric nature of existing payments regulation. The first is related to operational risk and the current model of derivative regulation of nonbanks that provide services to banks outlined in Section III.B. The second possible challenge is related to the background banking regulation that applies to payment services, especially through the connection services layer.

The rise of nonbanks in the top three layers of the payment stack—platform, processing, and account services—has already resulted in a movement of significant amounts of information technology systems into the hands of nonbanks. The critical question with respect to nonbank participation in these layers is whether derivative regulation of these nonbank suppliers of processing and other services is appropriate if banks are no longer the primary architects and operators of their own processing and other information technology operations.

All payment services—no matter the technology or business plan—involve operational risks, including risks associated with errors or delays in processing, system outages, insufficient capacity, fraud, data loss and

leakage, and other cyber and physical security risks.[307] New entrants and incumbents alike have recently faced high-profile cyberattacks and other operational issues.[308]

Nonbank specialization in the top three layers of the payment stack represents a potential opportunity as well as a potential challenge. On one hand, it has the potential to reduce operational risks.[309] Technological changes, such as dynamic tokenization now available in mobile payments, for example, might enhance the security of payments by eliminating the need to transfer payment card details for in-person payments.[310] On the other hand, new vulnerabilities may not become apparent until a technological change is deployed in the marketplace at scale.[311] And specialization may also transfer certain risks from highly regulated banks to relatively unregulated providers,[312] or lead, with unpredictable consequences, to a newly fractured market composed of numerous banks and nonbanks in competition with one another.[313]

The rise of nonbanks could also mean that the background banking regulation that applies to payment services, including through the connection services layer of the payment stack, becomes less effective in mitigating both operational and financial risks associated with payment

---

307. Mills et al., *supra* note 9, at 32.

308. Cyber criminals took $81 million from the Bangladeshi central bank in February 2016, for example, exposing weaknesses in the SWIFT messaging network. Martin Arnold, *Financial Industry Faces Extreme Disruption in Payments*, FIN. TIMES (Sept. 26, 2016), https://www.ft.com/content/1b82a0e6-4f67-11e6-8172-e39ecd3b86fc. Some new entrants, including virtual currency exchanges and wallet providers have track records that would be unacceptable for banks and other traditional account service providers. *See* Matt Levine, *Proxy Fights and Mystery Trusts*, BLOOMBERG (Nov. 8, 2017, 8:45 AM), https://www.bloomberg.com/view/articles/2017-11-08/proxy-fights-and-mystery-trusts ("People often talk about blockchain technology as a way to make things—payments, securities ownership ledgers, etc.—more *secure*. But actually existing blockchain applications in the wild—the actual cryptocurrency system that are used to store millions of dollars' worth of value—have a security record that would cause any regular bank to shut down in disgrace." (emphasis in original)); *see also* FIN. STABILITY BD., *supra* note 1, at 53. Examples of mishaps, well-documented elsewhere, span the ecosystems of essentially all virtual currencies. *See, e.g.*, Levine, *supra* note 308 (noting the ubiquity of such failures, including a 2017 issue that made inaccessible nearly $280 million in Ethereum coins stored with the wallet provider Parity).

309. BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 2.

310. GOV'T ACCOUNTABILITY OFFICE, *supra* note 40, at 24.

311. *See FSOC Annual Report*, 2016 Fin. Stability Oversight Council 127, https://www.treasury.gov/initiatives/fsoc/Documents/2012%20Annual%20Report.pdf [https://perma.cc/JYA4-EFU4] (see charts).

312. *See* FIN. STABILITY BD, *supra* note 1, at 19, 39 ("Should innovative payment and settlement services grow into critical FMIs, general business losses have the potential to impair the provision of critical services and interfere with recovery or an orderly wind down.").

313. William Magnuson, *Regulating Fintech*, 71 VAND. L. REV. 1167, 1200 (2018) ("[C]oncentrated markets are not necessarily more susceptible to systemic risk than dispersed or disaggregated ones.").

services. To the extent that that the dependence of nonbanks on the connection services of banks decreases in the future (because, for example, they no longer need banks to access messaging and settlement services), the degree to which background banking regulation applies to payment services will also decrease.

But it is difficult to assess with any precision whether and to what extent the non-application of background banking regulation to payment services would raise substantive concerns. What we do know is that banking regulation is primarily intended to address risks that arise from activities other than bank-provided payment services.[314] It is true of course that regulators have an interest in ensuring that payment services are not risk vectors to other parts of the financial system and real economy, as outlined in Section II.B. But we have no sense today—with a payments market that is still very much bank-centric—whether banking regulation as such is required to address these concerns.

Take, for example, bank capital requirements. They are designed to address financial risks associated with fractional banking but they also provide the ancillary benefit of ensuring that funds held in payment accounts are secure and that payments are funded and made on time. Regulators have not had to consider what measure of capital, if any, would be appropriate in a payments market reliant primarily or entirely on nonbanks, which are not leveraged in the same manner as banks.

In broad contours, the basic alternative to the current derivative and background regulatory frameworks is to apply regulation more directly to technology and other nonbank companies, in what could amount to a significant reordering of risk management in banking regulation. There is no evidence today that the current regime is somehow inadequate, although it is possible that regulators will later determine that asymmetries in regulatory treatment between banks and their nonbank competitors have become unfair from an operational risk standpoint (e.g., if the derivative nature of processing-service regulation grants competitive advantages to nonbanks without commensurate regulatory benefits) or even from a financial risk standpoint (e.g., if the competitive dynamic imperils the value proposition of banks on a wide scale).[315]

---

314. The failure of a bank can of course harm not only the bank and its customers but may spread financial instability across the financial system and can result in significant external costs to the real (non-financial) economy and society. *See* RICHARD SCOTT CARNELL ET AL., *supra* note 209, at 55; Letter from THE CLEARING HOUSE PAYMENTS CO. L.L.C., on Proposed Strategy to Address Wholesale Payment Fraud, to Morten Linnemann Bech, CPMI Secretariat 6–8 (Nov. 28, 2017), https://www.theclearinghouse.org/-/media/new/tch/documents/advocacy/20171128_tch_comments_to_cpmi_on_wholesale_fraud.pdf [https://perma.cc/4NHA-6KA2].

315. *Cf.* WORLD ECON. FORUM, *supra* note 47, at 28.a

At least one possible mechanism for realignment would be to broaden the scope of existing banking regulation. This might result, for example, in the targeted application of requirements usually associated with banking regulation, such as deposit insurance[316] or capital requirements, or in broader efforts to bring additional payment providers into the bank regulatory framework.[317] Nonbanks would presumably receive, in exchange, a number of benefits, including the ability to provide a broader range of financial services and access to messaging and settlement systems.[318] This is one of the potential implications of the OCC's proposal to establish a national charter for certain special purpose banks, at least if the charter would provide a basis for access to Fedwire and other Federal Reserve-operated messaging and settlement services.[319]

D. Serve as a Catalyst of Innovation to Correct Market Coordination Problems

Financial regulators and market participants have shared incentives to make at least some type of payments faster, cheaper, and more secure. But the fragmented nature of the payments market has made coordination

316. *See* DONG HE ET AL., *supra* note 157, at 33.

317. *See* FASTER PAYMENTS TASK FORCE, *supra* note 6, at 22 ("Key considerations in managing this [settlement] risk include . . . which risk mitigation measures are appropriate, such as pre-funding and capital requirements . . . .").

318. *Cf.* Mann, *supra* note 19, at 971 (arguing that "all entities that have access to the . . . settlement systems should be included" in a regulatory framework and "the principal regulatory activity [to ensure the financial stability of payment systems] should be to ensure the maintenance of a level of liquidity commensurate with the types of payment operation in which the entities engage").

319. At the federal level, the OCC has proposed a special purpose national bank charter that would apply a subset of existing banking rules to "financial technology companies." OFFICE OF THE COMPTROLLER OF CURRENCY, EVALUATING CHARTER APPLICATIONS FROM FINANCIAL TECHNOLOGY COMPANIES 2 (2017), https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf [https://perma.cc/BF7G-DXA2]. Under the charter, a special purpose national bank would be able to engage nationally in a limited range of banking activities, not including the taking of federally insured deposits, eliminating the need to obtain licenses or other approvals in each state in which it does business. *See id.* The OCC proposes to apply the same basic criteria and qualification requirements that are generally applicable to all special purpose national banks, while acknowledging that it "may tailor certain criteria as appropriate." *See id.* (noting that the charter would permit the activities described in 12 C.F.R. 5.20(e)(l), not including deposit-taking). The OCC proposes to apply the same basic criteria and qualification requirements that are generally applicable to all special purpose national banks, while acknowledging that it "may tailor certain criteria as appropriate." *See id*. at 8. The proposal indicates that the OCC would rely on traditional elements of bank evaluation, such as risk assessments records, systems, and controls; financial management, including capital and liquidity requirements; and requirements for contingency and recovery plans. *See id.* at 12.

among stakeholders difficult.[320] This coordination problem may present opportunities for regulators to serve as catalysts for innovation.

From 2015 through 2017, the Federal Reserve's Faster Payments Task Force engaged in one such effort, working with a wide range of stakeholders to "identify and assess . . . approaches for implementing safe, ubiquitous, faster payments capabilities in the United States."[321] The Task Force issued final recommendations ranging from the relatively modest (such as a proposed expansion in the operating hours of the Federal Reserve's messaging and settlement services)[322] to the ambitious (such as a governance framework and rules for faster payments and other new payment services).[323]

The Task Force also solicited proposals from stakeholders for real-time payment systems. One of the proposals—for The Clearing House's Retail RTP service—was implemented in late 2017,[324] although the real-world consequences of other private-sector proposals and of the Task Force's recommendations remain unclear.

E. Foster Innovation in Low-Risk Activities

When financial change in payments does warrant a regulatory response, regulators may also have the opportunity to reduce the compliance burden on certain technologies or business models through a "regulatory sandbox" approach. Financial regulators around the globe are racing to highlight their willingness to consider tailored or reduced regulatory requirements for potential innovations across financial services. The most prudent of these approaches are typically limited to

---

320. *See Our Process*, FASTER PAYMENTS TASK FORCE https://fasterpaymentstaskforce.org/meet-the-task-force/our-process/ [https://perma.cc/5JFH-TGXF] (last visited Oct. 2, 2018).

321. *About the Faster Payments Task Force*, FEDPAYMENTS IMPROVEMENT, https://fedpaymentsimprovement.org/faster-payments/about-the-task-force/ [https://perma.cc/GJ6J-MT3F] (last visited Oct. 2, 2018).

322. *See* FASTER PAYMENTS TASK FORCE, *supra* note 6, at 31, 33, 41.

323. *See id.* at 35–38. At the time of publication, the Federal Reserve Board was seeking public comment on potential actions to improve payment settlement, including the development by the Federal Reserve Banks of "a service for 24x7x365 real-time interbank settlement of faster payments" or "a liquidity management tool that would enable transfers between Federal Reserve accounts on a 24x7x365 basis to support services for real-time interbank settlement of faster payments." FED. RESERVE BD., POTENTIAL FEDERAL RESERVE ACTIONS TO SUPPORT INTERBANK SETTLEMENT OF FASTER PAYMENTS, REQUEST FOR COMMENTS 1, 1 (2018), https://www.federalreserve.gov/newsevents/pressreleases/files/other20181003a1.pdf [https://perma.cc/N5FN-VCAM].

324. *See* THE CLEARING HOUSE PAYMENTS CO. L.L.C. & FIS, PROPOSAL TO FASTER PAYMENTS TASK FORCE (2016), https://fasterpaymentstaskforce.org/wp-content/uploads/tch-fis-vs.pdf [https://perma.cc/TX8S-F3GN]; *see also supra* Sections II.E, II.F.

circumstances where there is uncertainty as to whether existing regulation can neatly apply to a potentially innovative technology or business model, the activity does not appear to alter the risk profile of the service, and the activity has not reached significant market penetration.[325]

Beyond assessing the relative risk profile of a potential innovation, it is also important to consider the effects that any new regulatory distinction may have on the competitive landscape. Sandboxes would seem most effective, for example, where they promote incentives that support stable business models of both new entrants and incumbents[326] or where diversification otherwise improves financial system resiliency.[327] They may have unintended consequences, however, if they artificially lower the compliance burden for some but not all suppliers[328] without any associated regulatory benefit, leading to regulatory escape and worsening regulatory outcomes. For that reason, regulators should consider whether a generally applicable change in regulation—rather than reduced compliance burdens for some—is more appropriate.

F. Leverage Financial Change that Reinforces Regulatory Objectives

The last potential regulatory strategy considered in this Article, one that is likely available across the payment stack, is to leverage aspects of financial change that may improve regulators' ability to uphold their regulatory and supervisory mandates. Opportunities to leverage the enhanced transparency of certain technologies could prove particularly valuable. That enhanced transparency may improve the ability of regulators to perform their duties and reduce information asymmetries among market participants.[329]

With the vast amount of data that is now transferred, processed, and stored in order to send and receive payments and to provide other financial services, regulators today face significant questions with respect to the collection and analysis of regulation-relevant information.

---

325. *See* BIS/CPSS, INNOVATIONS IN RETAIL PAYMENTS, *supra* note 6, at 53 ("As innovations tend to be small at the outset and may not go beyond a pilot phase, it can be difficult for central banks to assess a priori the potential of new products or processes as a basis for deciding on work priorities."); *id.* at 55 ("Another challenge is to determine when to apply oversight or regulations to a particular innovation. If applied too early, oversight might choke off innovation; if applied too late, it may subject the system to the related risks."); Bradley, *supra* note 248, at 85–89 (discussing "sandboxes" as a regulatory approach).

326. *See* FIN. STABILITY BD., *supra* note 1, at 13.

327. *See id.* at 13, 16–17.

328. *See* BIS/CPMI, NON-BANKS IN RETAIL PAYMENTS, *supra* note 11, at 17–18.

329. *See* FIN. STABILITY BD., *supra* note 1, at 13.

What information is relevant to their regulatory mandates? When must regulated entities provide access to extensive, real-time data, and when are summary reports enough? Who should have primary responsibility for analyzing data? Should regulated entities have that responsibility or should they instead provide bulk data to regulators? And when should regulators permit the outsourcing or consolidation of regulatory compliance functions to service suppliers in the processing layer of the payment stack?

The case of law enforcement regulation in payment services is illustrative in sorting through these types of emerging questions and the potential benefits of technology in achieving regulatory objectives. Today, when it comes to anti-money laundering and counter-terrorism financing compliance, account service providers have primary responsibility for analysis of bulk data.[330] Market participants have argued, however, that in some circumstances account providers should be able to engage processing service suppliers to collect customer information as part of their customer identification and due diligence programs.[331] These "compliance utilities" would collect and store customer due diligence information in a shared repository, to facilitate compliance with law enforcement regulation.[332]

Market participants have also suggested that regulators should allow account service providers in the third layer of the payment stack to provide bulk data on suspicious activity to regulators rather than expending resources on creating summaries of that data.[333] From a regulatory perspective, access to bulk, real-time information would require embedding additional expertise within regulatory agencies, the development of highly sophisticated surveillance tools, increased investment in data analytics resources,[334] and a feedback mechanism to

330. *See, e.g.*, Letter from Angelena Bradfield, Vice President & Senior Policy Specialist, AML/CFT & Prudential Regulation, The Clearing House Ass'n L.L.C. & Richard Foster, Senior Vice President and Senior Counsel for Regulatory and Legal Affairs, Fin. Servs. Roundtable, to U.S. Dep't of the Treasury 16 (July 31, 2017) [hereinafter Letter on Review of Regulations], https://www.theclearinghouse.org/-/media/tch/documents/tch-weekly/2017/20170731_joint_trades_comment_letter_to_treasury_on-review_of_regulations.pdf [https://perma.cc/ES8T-6GDY].

331. *See, e.g.*, *id.* at 6; THE CLEARING HOUSE PAYMENTS CO. L.L.C., A NEW PARADIGM: REDESIGNING THE U.S. AML/CFT FRAMEWORK TO PROTECT NATIONAL SECURITY AND AID LAW ENFORCEMENT 19–20 (2017).

332. *See* COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, BANK FOR INT'L SETTLEMENTS, CORRESPONDENT BANKING 19–22 (2016) [hereinafter BIS/CPMI, CORRESPONDENT BANKING], https://www.bis.org/cpmi/publ/d147.pdf [https://perma.cc/57V8-MASD]. A handful of foreign governments are developing their own centralized databases to streamline compliance. *See id.* at 29–31.

333. See Letter on Review of Regulations, supra note 330, at 16.

334. *See id.*; FIN. STABILITY BD., *supra* note 1, at 3 ("Supervisors and regulators should

correct errors and improve targeting of regulatory-relevant information at each payment provider.[335]

If this example is representative, regulators may need to consider acquiring new expertise and resources as they seek to leverage the potentially pro-regulatory benefits of financial change in payment services.[336]

CONCLUSION

The payment stack model constructed in this Article has shown that payments regulation is largely technology-neutral and activity-based, meaning that it is well-placed to adapt to financial change. Despite the pace of financial change in the payments market, the question that faces payments regulators is not, then, whether to engage in a wholesale rethinking of their approaches but how to focus their resources on fact-specific strategies. Going forward, the payment stack model can serve as a framework for identifying tailored regulatory responses and blunting calls for responses where financial change does not warrant them

---

consider placing greater emphasis on ensuring they have the adequate resources and skill-sets to deal with FinTech."). The Federal Reserve, the European Central Bank, and the Bank of England have, for example, each begun to use data "heat maps" to identify issues of regulatory concern from automated analyses of data produced by financial services companies. *See generally* INT'L MONETARY FUND, FIN. STABILITY BD. & BANK FOR INT'L SETTLEMENTS, ELEMENTS OF EFFECTIVE MACROPRUDENTIAL POLICY (2016), https://www.imf.org/external/np/g20/pdf/2016/083116.pdf [https://perma.cc/CL35-EHZB].

335. FIN. STABILITY BD., *supra* note 1, at 2–3.

336. Another instructive example is DLT, which has the potential to enable greater transparency, due to the shared nature of a DLT ledger, which means that all copies of a ledger are updated in real-time as transactions are validated. *See* GOV'T ACCOUNTABILITY OFFICE, *supra* note 40, at 44. Network participants could design DLT ledgers so that they provide financial regulators with shared, simultaneous, and automatic access to information necessary to carry out their regulatory mandates. *See id.*; IOSCO RESEARCH REPORT, supra note 276, at 59 ("Many DLT proponents note that one of the benefits of DLT is that regulators can participate as one of the nodes in the DLT, thereby having automated access to all the data. This in turn would allow regulators to have more complete and more traceable, real[-]time records."). Or regulators might even become gatekeepers to decentralized ledgers, providing connection services in place of or together with banks. Embedding regulators into a DLT network in these ways would essentially write regulation into the code of a payment system. Lawrence Lessig noted this possibility of "code as regulation" in 1996. *See* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408 (1996). Implementing these ideas and others like them will quickly give rise to complicated questions, however, involving the scope of information sharing and aggregation, appropriate access permissions, and compliance with data protection and data privacy rules. BIS/CPMI, CORRESPONDENT BANKING, *supra* note 332, at 31. Market participants using a common ledger would presumably agree on the type and degree of information to be shared with regulators, with respect to each transaction and each customer, taking into account privacy laws and other regulations in each jurisdiction in which the DLT network operates. *See* Mills et al., *supra* note 9, at 25. But this could result in the application of the most restrictive regulations across the entire network, potentially limiting the usefulness to regulators.